CHAPITRE 8

Tout individu plongé dans l'erreur, subit une poussée verticale dirigée de haut en bas qui l'y enfonce un peu plus.

Philosophe Grec anonyme du Deuxième siècle.

RACHEL, SEMIRAMIS et ARCHIMEDE

Les opérations RACHEL, SEMIRAMIS et ARCHIMEDE, menées depuis 1988 pour le compte de la Direction Générale de l'Aviation Civile, avaient pour objectif une meilleure compréhension du rôle des erreurs humaines dans la genèse des accidents aériens. Ces trois opérations sont décrites en détail dans le numéro 153 d'Aéronautique et Astronautique.

Le fichier **RACHEL** (**R**épertoire d'**A**nalyse du **C**omportement **H**umain **E**n **L**igne) rassemble des accidents aériens survenus dans le monde occidental depuis 1973 jusqu'à 1987. Les renseignements de base sont fournis principalement par le fichier OACI (Organisation Mondiale de l'Aviation Civile) et le fichier de la CAA (Organisme britannique de certification).

Environ 500 accidents, dont pratiquement 450 utilisables, ont été analysés pour lesquels le facteur humain a joué un rôle dans la genèse de la catastrophe.

On a pu constater qu'il n'y avait pas d'accidents dus à une surcharge de travail ou du moins que ce type d'accident ne survient que lorsque l'équipage est incapable de faire face à une charge de travail normale pour des raisons de fatigue, d'états physiologiques anormaux, etc. (la période retenue pour la collecte est telle que les avions intéressés sont des avions modernes relativement bien équipés en automatismes soulageant l'équipage; ce ne sont toutefois pas les avions de la dernière génération dite des "glass-cockpit").

Ainsi la très grande majorité des accidents a pour origine des erreurs de représentation et une mauvaise évaluation du risque encouru.

Rappelons qu'une erreur de représentation est une erreur au cours de laquelle un opérateur et/ou l'ensemble de l'équipage se fait une fausse image de la situation et ne parvient pas à rétablir l'image réelle. Sa démarche de correction de la situation est cohérente avec l'image qu'il s'est bâtie, mais est en général mal adaptée à la réalité.

Le résultat le plus spectaculaire de l'analyse est le fait qu'il a été possible de regrouper la plupart des accidents en pratiquement sept familles. Certaines de ces familles sont typiques du travail aérien, mais on retrouve une famille du genre "Three Mile Island", le premier accident nucléaire aux Etats Unis, (erreur de représentation due à une présentation ambiguë de l'information) et une famille du genre "Tchernobyl" (successions de procédures improvisées sans évaluation du risque encouru).

Parmi les sept familles il a été possible de sélectionner quelques scénarios pouvant être reproduits au simulateur de vol.

Ainsi, à partir d'accidents réels, ont été bâtis des scénarios typiques reproduisant l'enchaînement des événements caractéristiques d'une famille. Les scénarios ont été adaptés au type d'avion simulé et aux lignes aériennes desservies par la compagnie française dont les équipages (volontaires) ont accepté de participer à l'expérience.

C'est alors que l'opération **SEMIRAMIS** (**S**ystème pour l'**E**tude des **M**odèles **I**nternes de **R**eprésentation et **A**nalyse des **M**éthodes d'**I**nterprétation de **S**ituations) a été mise sur pied, avec l'aide d'AEROFORMATION, (devenu depuis Airbus Training) pour ajuster les méthodes d'essais. A cette occasion ont été bâtis les programmes permettant de relever en cours de simulation les paramètres de vol et les commandes de l'équipage, et de les restituer sur l'écran d'un micro-ordinateur sous la forme, soit d'un tableau de bord reconstitué, soit de la trajectoire vue en plan ou en perspective. Au cours de cette opération est apparue aussi l'utilité de l'enregistrement vidéo et phonie des trois membres de l'équipage et de l'enregistrement de leurs rythmes cardiaques pour estimer le réalisme de la simulation.

La visualisation du tableau de bord et de la trajectoire, ainsi que les enregistrements vidéo et phonie, étaient présentés aux équipages, juste après l'essai, de façon à provoquer leurs remarques sur les événements enregistrés et surtout afin d'obtenir de leur part des commentaires sur les raisons qui les avaient poussés à prendre telle ou telle décision (bonne ou mauvaise). Le fait de leur présenter le déroulement de l'action sous une forme très imagée, leur permettait en général de se replacer dans le contexte psychologique du vol et de se remémorer le déroulement de leur démarche intellectuelle de prise de décision. Nous avons pu ainsi, plusieurs fois, reconstituer la succession des raisonnements ayant conduit à une erreur, niée a priori parce que non remarquée, et mise en évidence par la relecture. Nous insistons sur la nécessité d'une telle présentation imagée. La présentation de l'événement sous forme de courbes permet de reconnaître l'erreur, mais beaucoup plus difficilement d'en faire reconstituer la genèse par l'opérateur. Il faut replacer l'équipage dans des conditions psychologiques voisines de la réalité pour l'aider à se remémorer la succession des événements et des décisions.

Une fois l'outil mis au point, la société APSYS (Aérospatiale Protection Systèmes) a lancé l'opération **ARCHIMEDE** (**A**ction de **R**echerche sur le **C**omportement **H**umain en **I**ncident, **M**éthode d'**E**valuation et de **D**étection des **E**rreurs) sous la forme de deux campagnes de douze vols simulés. Chaque vol de quatre heures environ comprenait des séquences destinées à mettre les équipages dans les conditions psychologiques du vol pour faire oublier la simulation (mise en route au parking, roulage, décollage, montée, croisière avec quelques pannes ou incidents mineurs) et plusieurs séquences reproduisant des scénarios tirés d'accidents types réels (deux séquences, prises parmi quatre scénarios, pour la première campagne, sept séquences pour la deuxième campagne).

Le souci de réalisme a été poussé jusqu'à demander aux équipages de porter l'uniforme et à reproduire l'environnement radio (en passant des enregistrements de trafic réels effectués dans les zones correspondants aux trajectoires simulées et en faisant intervenir un contrôleur aérien simulant le trafic radio avec l'équipage et d'autres équipages joués par les ingénieurs d'essai).

Les équipages ont tous reconnu le réalisme de la simulation, confirmé par les enregistrements des rythmes cardiaques. Ils ont également noté que les scénarios étaient très conformes à la réalité d'un vol et ils n'ont pas eu l'impression d'avoir été "piégés" par des événements anormaux que l'on ne pourrait rencontrer en vol.

Le résultat des essais n'a pas été conforme à nos prévisions. Nous pensions observer un ou deux cas de déviation intéressants dans les quelques cent scénarios exécutés.

Or chaque scénario a provoqué quasi systématiquement des déviations plus ou moins importantes, proches de l'accident.

Les événements, dont la succession conduit à cette situation critique sont d'une extrême banalité (petites erreurs courantes commises très souvent mais la plupart du temps corrigées très rapidement ou sans conséquences dans le contexte et, par suite, rarement notées par les équipages).

C'est l'enchaînement malencontreux de ces erreurs qui est rare, mais non l'occurrence de chaque erreur.

Le rôle des scénarios était justement de provoquer cet enchaînement malencontreux en favorisant une erreur au mauvais moment ou en interdisant la correction par un événement extérieur, réaliste, judicieusement provoqué.

Par exemple, l'équipage attendait le passage à la verticale d'une balise à un instant calculé en tenant compte du vent donné par la météo. Un vent légèrement supérieur à la prévision retardait l'avion. Au moment attendu, un éclair provoquait fugitivement une fausse indication de passage de la balise (la situation orageuse était simulée par de la turbulence et des éclairs, donc non ignorée par l'équipage). Au même instant le contrôle de trafic aérien demandait au pilote d'annoncer le passage de la balise. Cette simultanéité d'événements poussait en général l'équipage à se croire à la verticale de la balise et à commencer trop tôt sa descente dans une région montagneuse, avec le risque évident de percuter le relief. On notera que c'est la conjonction, rare mais provoquée par la simulation, de nombreux événements, erreurs d'estimation du vent, éclair à l'instant prévu du passage de la balise, mauvaise indication du récepteur de la balise, trafic radio, relief qui conduit à une situation dangereuse, alors que chaque événement est banal et relativement fréquent.

Il faut noter toutefois que l'un des scénarios n'a conduit aucun équipage à l'erreur. Il s'agissait d'un changement de piste juste avant le décollage. RACHEL a enregistré plusieurs cas réels d'équipage ayant oublié de recalculer les paramètres de décollage (alors que la longueur de la nouvelle piste et la direction du vent étaient

défavorables). Les consignes compagnie et la pratique des équipages appelés à travailler dans des régions où la météo provoque souvent des changements de piste au dernier moment ont permis à tous les équipages d'ARCHIMEDE d'exécuter les opérations de reconfiguration de l'avion, naturellement d'ailleurs et sans même avoir conscience du piège tendu.

Ces résultats ont conduit à consulter un fichier analogue à RACHEL mais répertoriant, non les accidents, mais les incidents graves.

L'analyse du fichier "Incidents" n'a pas fait apparaître de familles nouvelles. Les accidents ne seraient que des incidents qui ont "mal tourné", mais ne semblent pas être de nature différente. Ceci milite en faveur du recueil de ce type de données, car les incidents sont beaucoup plus fréquents que les accidents et plus facile à analyser, en particulier parce que l'équipage peut "s'expliquer". Malheureusement, la tendance fâcheuse consistant à considérer que les erreurs sont des fautes, rend encore difficile la divulgation de ces données fondamentales pour la sécurité.

Ainsi la grande majorité des équipages participant à l'opération, en conditions réalistes de simulation, mis dans les mêmes conditions, a commis les mêmes chaînes d'erreurs conduisant à la catastrophe. Les erreurs étaient toutes, prises séparément, extrêmement banales (et dans la plupart des cas normaux corrigées instantanément ou sans conséquences). Ce résultat est très encourageant car il est plus facile d'identifier et donc de tenter de contrer des phénomènes fréquents que d'intervenir sur des événements uniques, et très rares.

Par ailleurs, il semble bien que des procédures compagnie, claires et précises, bien intégrées par la pratique des équipages puissent permettre d'éviter quelques types de chaînes d'erreurs.

Enfin, de l'avis de tous les équipages ayant participé aux essais, ce type d'opération au simulateur est hautement instructif. Il permet à chacun de prendre conscience du fait que nul n'est à l'abri d'un enchaînement malencontreux, quels que soient sa compétence et son sérieux. Il permet également de reconnaître l'existence des erreurs de représentation et donc peut-être de les identifier en vol réel. Une réflexion est en cours pour orienter une partie des vols d'entraînement au simulateur dans cette direction analogue à celle déjà connue sous le vocable LOFT (Line Oriented Flight Training).

La mise au point d'un scénario type ARCHIMEDE nécessite plusieurs étapes.

⇨ confection d'une base de données rapportant des accidents ou des incidents rencontrés en vol opérationnel, en entraînement ou en formation au simulateur (Opération type RACHEL).

⇨ analyse de chacun des accidents/incidents de la base à l'aide de grilles adaptées et caractérisation de chacun d'entre eux par une chaîne d'événements (chaque événement est identifié par un premier code caractérisant le Facteur d'Erreur et un second code caractérisant le Défaut Système à l'origine du Facteur d'Erreur).

⇨ identification de chaînes ou de sous-chaînes d'événements semblables sinon communes à plusieurs accidents/incidents, chaînes rencontrées dans des conditions de vol analogues (telle chaîne au décollage ne peut être comparée à une chaîne, même analogue, en croisière haute altitude).

Cette opération permet de définir des familles typiques d'accidents/incidents caractérisées par une similitude au moins grossière des circonstances essentielles et de la ou des erreurs principales commises. Ces familles peuvent être à l'origine d'un scénario.

⇨ identification de chaînes ou de sous-chaînes d'événements que l'on pense être symptomatiques d'un type d'accident original. Là encore, ces chaînes peuvent être à l'origine d'un scénario.

⇨ si la chaîne identifiée peut être aisément simulée, élaboration d'un scénario sommaire provoquant une chaîne d'événements, analogue à la chaîne identifiée, dans le déroulement d'un vol compagnie type, c'est-à-dire dans le déroulement d'une mission bien connue des équipages. Parmi les conditions de faisabilité d'un scénario, il y a lieu d'examiner si le scénario de base est très dépendant du type d'avion ou si, à des adaptations de détail près, il peut être considéré comme général.

⇨ élaboration d'un "script" détaillé décrivant le minutage précis des opérations à effectuer :

- par le responsable du simulateur (mise en place des événements externes, tels que turbulence, gradients de vent, perte de visibilité ou des événements internes, tels que pannes de systèmes ou d'instruments de bord),
- par le responsable de l'ATC (Air Traffic Control ou Contrôle de la Navigation Aérienne), (teneur des messages, variantes en fonction des réponses prévisibles de l'équipage, changement des fréquences radio, etc.),
- par le responsable de la simulation du trafic radio d'autres avions (messages, codes d'identification, réponses ou demandes à l'ATC, etc.).
- par le responsable de l'essai (rôle de coordination de tous les acteurs) en particulier en cas de réactions possibles, mais non attendues, de l'équipage.

Le script est tout d'abord minuté en calculant les performances de l'avion, puis vérifié par quelques essais au simulateur. Cette opération au simulateur permet en outre d'entraîner les divers responsables et peut conduire à corriger ou changer des opérations n'apparaissant pas comme réalistes à l'expérience.

⇨ Enfin, essai du scénario au simulateur avec un équipage qui en ignore le contenu, mais dont le rôle est d'en faire la critique après exécution. L'expérience montre qu'en général deux essais au moins sont nécessaires, le premier ayant fait apparaître des événements imprévus et mis en évidence des erreurs de minutage.

Ainsi, chaque scénario, représentatif d'une famille, est bâti en se référant à un accident réel, en ne modifiant que les circonstances imposées, par exemple, par le type d'avion ou les caractéristiques de la compagnie à laquelle appartiennent les équipages (procédures compagnie, lignes aériennes et terrains desservis, etc.).

Citons les cas retenus pour l'opération ARCHIMEDE (l'erreur la plus caractéristique est citée, mais notons que le scénario ne "fonctionne" que si d'autres événements interviennent).

⇨ en cours de descente, la procédure d'approche étant déjà engagée, déroutement, pour raisons météo, aidé par guidage radar. Au moment où le Contrôle de Trafic Aérien donne l'autorisation de descendre sur la balise d'entrée du terrain de déroutement et cesse la surveillance radar; l'équipage trompé par les quelques changements de route précédents se fait une mauvaise estimation de la position de l'avion et entame, sans précautions, la descente dans une région accidentée (erreur de représentation sur la position de l'avion, en plan et en altitude, provoquée par la succession des événements précédant la descente). (Voir au chapitre 7 l'accident du B727 de TWA accidenté le 1-12-74 à Berryville aux environs de l'aéroport de Washington Dulles)

⇨ la procédure d'atterrissage sur un terrain dans une zone montagneuse prévoit, après passage à la verticale d'une balise sur l'axe d'approche, l'entrée dans un hippodrome d'attente. Le temps est orageux, le vent supérieur au vent météo retarde quelque peu l'avion. A l'heure prévue de passage de la balise, le Contrôle de Trafic Aérien demande confirmation de position ce qui amène le pilote aux commandes à regarder le radiocompas. A ce même instant la foudre dans un cumulo-nimbus derrière l'avion provoque le basculement de l'aiguille. Le pilote se croit à la verticale de la balise et entame le virage de procédure, dans une région dangereuse (erreur de représentation sur la position de l'avion provoquée par la conjonction de plusieurs événements aléatoires, appel du Contrôle de Trafic Aérien, retard sur les prévisions, basculement intempestif du radiocompas.). C'est ce scénario que nous avons utilisé plus haut comme exemple.

⇨ l'avion est en vue de la piste (bonne météo) lorsque le Contrôle de Trafic Aérien donne l'autorisation d'atterrissage, mais il est mal placé (trop haut, trop près, trop vite). Le commandant de bord décide de tenter l'atterrissage (alors qu'aucune urgence ne le pousse à le faire, sinon le désir de se retrouver au sol !) et tarde à remettre les gaz (et même poursuit une approche scabreuse) (Erreur d'estimation du risque). (Scénario dit d'Approche Précipitée)

⇨ l'avion se présente en finale sur la piste de gauche, lorsque le contrôle demande l'atterrissage sur la piste de droite (plus courte et dont le seuil est en retrait par rapport à la piste de gauche). La manœuvre de baïonnette est théoriquement possible mais délicate à exécuter en toute sécurité. Certains pilotes tentent la manœuvre plutôt que d'exécuter une remise de gaz. A cette occasion se pose le problème de la décision de remise de gaz et de l'exécution de la manœuvre suivant qu'elle est décidée par l'équipage ou imposée par la tour.

⇨ un cisaillement de vent au décollage n'est pas prévu par l'équipage malgré les informations météo (déplacement d'une zone orageuse autour du terrain, variations rapides du sens et de la direction du vent). La procédure adaptée (utilisation préventive de la poussée maximale au décollage, maintien de l'assiette malgré la chute de la vitesse indiquée pour éviter a tout prix la perte d'altitude) n'est pas appliquée, le phénomène n'étant pas identifié correctement; (erreur de représentation par méconnaissance du phénomène).

⇨ la prise de pression totale de l'anémomètre (l'indicateur de vitesse) du pilote aux commandes est bouchée par un corps étranger. Il en résulte une augmentation de la vitesse indiquée par l'anémomètre au cours de la montée suivant le décollage (la pression statique diminue avec la prise d'altitude et la différence totale - statique augmente, ce qui se traduit par une augmentation de vitesse indiquée). Le pilote non aux commandes est perturbé par diverses demandes du Contrôle de Trafic Aérien (changement de fréquences radio, demande de prévisions, changement de procédure de montée, etc.) ce qui l'empêche de surveiller les paramètres de vol. Le pilote aux commandes augmente l'incidence pour contrer l'augmentation intempestive de la vitesse. (Erreur de représentation due à une fausse information). Une fois constatée la différence d'indication des deux badins,

suit une période de discussion au sein de l'équipage pour déterminer quel est l'instrument qui fournit une valeur correcte.

⇨ l'horizon artificiel du pilote aux commandes se bloque (panne mécanique non détectée sur certains avions de la génération 70-90). Le pilote non aux commandes est perturbé par les demandes du Contrôle de Trafic Aérien et ne note pas la dérive de l'assiette latérale. Dans quelques cas, une fois l'anomalie détectée, ce qui peut prendre de longues secondes si le pilote suit le directeur de vol, le pilote attribue à une panne des commandes de vol et non à une panne de l'instrument, la non-réponse à ses actions au gauchissement.

⇨ pendant le roulage avant décollage, la tour propose un changement de piste (la piste proposée est plus courte et orientée vent de travers). L'équipage accepte et ne recalcule pas le carton de décollage ce qui l'amène à des vitesses de décision, de lever de roulette et de montée initiale erronées n'assurant pas la sécurité au décollage. Il ne reconsidère pas la configuration d'hypersustentation qu'il faut éventuellement envisager (erreur d'organisation conduisant à un non-respect des procédures).

Ce scénario, représentatif d'une dizaine d'accidents réels, n'a donné lieu à aucune erreur de la part des douze équipages. L'explication de ce fait, surprenant a priori, en est que les équipages de l'ancienne compagnie UTA, qui participaient à ces essais, rencontraient ce type de situation au cours de leurs missions en Afrique où les changements brutaux de météo imposent très souvent des changements de piste au dernier moment.

⇨ en début de montée, le pilote passe le pilote automatique sur le mode "maintien de la vitesse indiquée" (IAS HOLD). Il est au même instant perturbé par le Contrôle de Trafic Aérien et ne note pas que le mode IAS HOLD saute et que c'est le mode VERTICAL SPEED (maintien de la vitesse verticale) qui est mis en service (extinction du voyant IAS HOLD et allumage du voyant, voisin, VERTICAL SPEED). Au cours de la montée la vitesse indiquée régresse (pour maintenir la vitesse verticale constante). Le phénomène est aggravé par du givrage. Enfin des vibrations moteurs (dans les tolérances acceptables néanmoins) viennent perturber les trois membres d'équipage et détourner leur attention des performances de l'avion. (Erreur de représentation par manque d'analyse de la situation; le pilote a mis le pilote automatique sur IAS HOLD, l'a vu s'afficher et ne vérifie plus si ce mode est toujours en service; non-renouvellement de l'image mentale de la situation). Ce type de scénario préfigure les scénarios que l'on risque de rencontrer avec les avions modernes glass cockpit fortement automatisés (mauvaise connaissance du fonctionnement des automatismes, mauvaises prises d'information sur l'état des automatismes). (voir le paragraphe décrivant les boucles de contrôle de la machine en utilisant les automatismes au chapitre 4; voir au chapitre 7 l'incident survenu au-dessus de Luxembourg le 11-11-79 au DC10 d'Aeromexico.)

Il faut enfin noter que tous les scénarios rencontrés dans la réalité ne peuvent pas être simulés. Pour pouvoir être simulé, un scénario doit reposer sur une chaîne d'événements dont chacun peut être provoqué par une action extérieure de la part du Contrôle de Trafic Aérien perturbant l'équipage au "bon" moment, du responsable du simulateur introduisant une panne à un instant crucial, de la part du responsable du trafic radio émettant un message ambigu, etc. Si la chaîne contient une interprétation erronée d'un message, d'un paramètre de vol, il est évident qu'un tel événement ne peut être provoqué. L'expérience ARCHIMEDE a toutefois montré que de tels événements se produisent spontanément, mais on ne peut compter sur ce hasard pour bâtir un scénario valable.

ARCHIMEDE n'est qu'une première tentative pour nous plonger dans le bain (ou plutôt l'océan) des erreurs humaines. Il nous reste encore beaucoup à faire avant de pouvoir en émerger en criant EUREKA.

D'après Tex Avery

CHAPITRE 9

Si tu laisses la porte fermée à toutes les erreurs, la vérité n'entrera pas.
Rabindranâth Tagore

Il n'y a rien de plus difficile à entreprendre, de plus périlleux à poursuivre et de plus incertain à réussir que d'introduire un nouvel ordre des choses, car l'innovateur a pour adversaires tous ceux qui ont réussi dans les conditions anciennes et ne trouve qu'une aide tiède auprès de ceux qui pourront réussir dans les nouvelles.
Nicolo Macchiabelli (1469-1527)

Ne pas frapper de dérision les actions humaines, ne pas les déplorer, ne pas les maudire, mais les comprendre.
Spinoza

QUELQUES REFLEXIONS SUR LE RETOUR D'EXPERIENCE

Depuis les années cinquante les responsables du transport aérien se préoccupent de mettre en place les moyens nécessaires à l'amélioration de la sécurité des personnes transportées et des personnes survolées. Le résultat de ces efforts est évident. La probabilité d'accident par vol a été divisée par un facteur voisin de mille au cours des quatre dernières décennies. Il n'en reste pas moins que cette amélioration de la sécurité s'essouffle et qu'il semble bien que l'on soit parvenu à un plancher. Les derniers apports de la technologie, reposant sur l'utilisation d'automatismes fiables et performants, inclinent quelque peu ce plancher dans un sens bénéfique, mais nous nous heurtons au problème sérieux de l'erreur humaine.

La recherche de l'amélioration de la sécurité est permanente dans tous les domaines de l'industrie de production et dans l'industrie des transports. Elle n'a pas suivi les mêmes voies que dans le transport aérien pour des raisons diverses. Citons trois exemples. Nous les avons déjà évoqués au chapitre 1.

Dans l'industrie de production d'énergie nucléaire, l'assurance de sécurité reposait, jusqu'à la fin des années soixante-dix, sur l'étude de l'incident technologique le plus grave que l'on pouvait raisonnablement imaginer. Si la rupture d'une canalisation principale du circuit de génération de vapeur pouvait être maîtrisée sans conduire à la catastrophe, la sécurité était assurée. L'erreur humaine était considérée comme impossible grâce à une formation poussée des opérateurs. L'accident de Three Mile Island a montré, en 1979, que ces hypothèses étaient fausses. Un incident d'une grande banalité n'a pu être maîtrisé par suite d'une erreur humaine provoquée par une erreur de conception du pupitre de contrôle.

Dans le transport ferroviaire, la sécurité reposait sur le respect des procédures qui, pensait-on, couvraient tous les cas possibles. L'erreur humaine était jugée comme impossible puisque les opérateurs étaient formés pour appliquer des consignes simples qu'ils devaient connaître par cœur et qu'ils se devaient d'appliquer puisqu'ils connaissaient par ailleurs les punitions encourues en cas de non-application. Tant que le réseau ferroviaire a été relativement simple, cette hypothèse du respect des procédures s'est révélée efficace. Mais les accidents survenus au cours des années quatre-vingts, Flaujac, Argenton sur Creuse, Gare de Lyon, Gare de l'Est en ont montré les limites. Les opérateurs n'ont pas su ou pas pu appliquer des procédures qu'ils connaissaient parfaitement.

Dans le transport maritime, en particulier dans le domaine du transport passagers et véhicules, la sécurité reposait sur le respect des consignes assuré par la discipline bien connue des gens de mer. Là encore l'accident du Herald of Free Enterprise en mer du Nord a montré les limites de cette hypothèse. L'ensemble de la corporation a été bouleversé par le fait qu'un marin aussi expérimenté et soucieux de la sécurité que l'était le commandant de ce navire ait pu commettre l'erreur d'appareiller avec une porte ouverte sur le pont hangar des véhicules.

Chacune de ces industries a donc décidé de se pencher sur le problème de l'erreur humaine qui de toute évidence limite les améliorations de sécurité qu'impose la morale et que réclame l'opinion publique qui ne supporte plus l'accident comme une fatalité incontournable.

Certains esprits audacieux envisagent de supprimer l'homme dans le contrôle des véhicules, du trafic ou des systèmes de production. Indéniablement, cette solution éliminera les erreurs humaines, du moins les erreurs de pilotage et de guidage. Elle n'éliminera pas toutefois les erreurs de conception. Par ailleurs, supprimer l'homme au profit des automatismes suppose une connaissance exhaustive de toutes les circonstances que l'on peut rencontrer

au cours des opérations. Nous n'en sommes pas là, il s'en faut de beaucoup, et nous ne pouvons pas, pour l'instant, nous passer des facultés fondamentales de l'homme, capacité de reconnaissance de situations non prévues et capacité de décision reposant sur des critères qualitatifs et non quantitatifs. La présence de l'homme est sans conteste une cause d'accident, mais nous ne pouvons nous en passer car l'homme est le seul capable de faire face à l'imprévu. Il faut d'ailleurs noter que les statistiques ne nous donnent que les cas où l'homme s'est montré cause d'accident et jamais les cas où l'homme a évité l'accident grâce à ses qualités.

D'aucuns rappellent que certains trains, le VAL par exemple, circulent sans conducteur. Ils utilisent cet argument pour montrer que l'on peut se passer de l'homme et le remplacer par des automatismes. Certes, il n'y a pas d'opérateur à bord du véhicule, mais il y a un homme dans la boucle au centre de contrôle du système. C'est lui qui prendra les décisions en cas d'événement imprévu, la sécurité étant facilitée du fait qu'il est toujours possible d'interrompre le trafic et d'arrêter le véhicule en attendant l'arrivée des secours ou des dépanneurs. Il est évident que cette solution est difficilement applicable au transport aérien où seul l'homme à bord peut intervenir.

Pour tous les systèmes qui peuvent être bloqués quasi instantanément par une manœuvre du type arrêt d'urgence, il est possible d'envisager une automatisation complète. La sécurité repose alors sur l'hypothèse qu'en cas de défaillance des automatismes (pannes ou situation imprévue rendant inefficace un automatisme) un dernier automatisme de conception simple déclenche l'arrêt d'urgence.

De tels systèmes sont rares et nous sommes dans la situation, pour l'instant inévitable, où nous devons utiliser l'homme dans les boucles de contrôle des grands systèmes, car il est indispensable pour assurer la sécurité dans les cas imprévus. Mais nous devons éviter de le mettre dans des situations pour lesquelles il est mal adapté et sujet à l'erreur.

Il nous faut donc améliorer nos connaissances en matière d'erreur humaine et identifier soigneusement les circonstances qui favorisent les dysfonctionnements des opérateurs.

Seule une analyse du comportement des opérateurs en service nous permettra de dégager les circonstances critiques conduisant à l'erreur et trouver des remèdes pour limiter l'apparition de ces circonstances néfastes.

C'est l'objet du **RETOUR D'EXPERIENCE**.

Ce terme de retour d'expérience recouvre de nombreuses acceptions et est utilisé pour caractériser des opérations de nature très différentes.

Dans de nombreuses industries, le retour d'expérience a pour objet de recenser les défaillances des matériels en service afin d'améliorer leur fiabilité (souci de sécurité et surtout souci d'amélioration de la régularité de fonctionnement). L'objectif est quelquefois de déterminer les opérateurs à risque pour les écarter des fonctions de responsabilité.

Dans le domaine de la chimie le retour d'expérience a pour objet l'étude du comportement de l'installation de production après un incident grave ou un accident, par exemple évolution d'une nappe de gaz ou de fluide toxique après rupture des réservoirs ou réactions chimiques se développant dans les produits s'échappant intempestivement des réacteurs. Ces études sont manifestement utiles pour la sécurité (il est difficile de modéliser ces phénomènes sans contrôler le modèle par une expérience qu'on ne peut raisonnablement provoquer volontairement), mais elles ne correspondent pas à notre objectif.

Dans de nombreux cas, les responsables du retour d'expérience ne s'intéressent qu'aux accidents majeurs ayant entraîné destructions importantes et pertes de vies humaines. L'objectif est alors de trouver "la cause", dite majeure, de l'accident, c'est-à-dire la dernière erreur de l'opérateur, et de trouver une parade, sous forme en général d'une modification technologique importante, permettant d'affirmer qu'une telle catastrophe ne se reproduira plus.

Les accidents sont très instructifs mais trop rares, heureusement, pour que l'expérience qu'ils fournissent soit suffisante pour améliorer nos connaissances en matière de comportement des opérateurs. En outre il ne s'agit pas de trouver une parade évitant la dernière erreur de l'opérateur. Celle-ci n'a en effet qu'un caractère anecdotique. Un autre opérateur dans les mêmes conditions aurait commis une autre erreur. Ce qu'il importe, c'est identifier les conditions dans lesquelles l'erreur a été commise et c'est trouver un moyen pour éviter que de telles conditions ne se reproduisent. En outre l'expérience montre qu'un accident n'est pas dû à un événement unique mais à une succession d'événements comportant des erreurs plus ou moins banales et, en général, sans conséquences. Il importe donc d'identifier cette séquence d'événements et les circonstances ayant conduit à leur apparition, car il est alors possible de trouver une parade limitant l'une de ces apparitions, et par conséquent limitant la probabilité de catastrophe.

Le retour d'expérience tel que nous le définissons pour couvrir notre objectif d'étude du comportement humain comporte donc les opérations suivantes :

- ⇨ Recueil des incidents ou accidents en service en identifiant les conditions dans lesquelles ils se sont déroulés. Par conditions nous entendons
  - les conditions "internes", par exemple composition, ancienneté, état physiologique (fatigue, maladie), état psychosociologique (soucis personnels, familiaux, professionnels ou événements heureux, naissance, gain à la loterie,..), etc. des membres de l'équipage.
  - les conditions "externes", vol de jour, de nuit, sans visibilité, en turbulence, présence d'instructeurs, de personnalités, mouvements sociaux, etc.
- ⇨ Analyse pour tout incident ou accident, de la succession des événements ayant conduit à une situation potentiellement dangereuse ou catastrophique en précisant, pour chacun de ces événements, les conditions ayant favorisé l'erreur.
- ⇨ Une fois un événement identifié, recherche du ou des défauts du système ayant créé les conditions favorisant l'erreur.
- ⇨ Lorsqu'un défaut système identifié participe à un nombre significatif d'incidents, recherche du ou des remèdes possibles pour l'éliminer ou en réduire les conséquences.

La connaissance des conditions dans lesquelles s'est déroulé un incident est importante car elle permet d'estimer la probabilité de se retrouver dans des conditions analogues et donc de donner un poids aux actions envisageables pour y trouver remède. Pour plaisanter, il n'est peut-être pas nécessaire de passer beaucoup de temps à l'analyse d'un incident qui s'est déroulé sur un avion de ligne, pendant la nuit de Noël, dans la turbulence d'un gros orage, en période de grève partielle du contrôle aérien, après dix heures de vol, avec le ministre des transports dans la cabine, un commandant de bord ancien en cours de divorce et couvant la grippe et enfin un tout jeune copilote dont l'épouse est sur le point d'accoucher !

Rappelons-le, il ne s'agit pas, comme pour une enquête d'accident, de dégager toutes les circonstances à l'origine de l'incident, mais d'identifier les circonstances sur lesquelles nous pouvons agir pour en réduire la probabilité d'apparition.

Nous avons dit qu'il faut agir lorsqu'un nombre significatif d'incidents a été détecté. Ce nombre significatif peut se réduire à l'unité si les conséquences potentielles de l'incident sont suffisamment graves et surtout lorsque l'on constate que la catastrophe peut être déclenchée à la suite d'une seule erreur humaine, car la probabilité d'erreur humaine est trop grande pour faire reposer la sécurité sur l'hypothèse que l'opérateur est suffisamment formé et entraîné pour éviter l'erreur.

Il faut se souvenir qu'un opérateur mal entraîné commet en moyenne une erreur pour cent actions. Un opérateur bien formé et bien entraîné commet une erreur sur mille actions. Un opérateur très habile, très entraîné et particulièrement chanceux ne commettra qu'une erreur sur dix mille actions. Mais cette fréquence est encore trop élevée pour que la sécurité soit assurée par le seul respect des procédures. Il est donc fondamental de détecter tous les incidents dus à une seule erreur d'opérateur et trouver des remèdes (détrompage mécaniques ou automatiques, systèmes d'avertissement, procédures de vérification par un autre opérateur, etc.). A titre d'exemple rappelons que lorsque sur notre ordinateur personnel nous tapons la commande "FORMAT A:", en général le message "Attention vous allez effacer tous les fichiers. Confirmez la commande." est affiché et nécessite la réponse "OUI" (Trois lettres à taper pour éviter la réponse réflexe !). Ce message de confirmation est bien utile si par mégarde nous avons tapé la commande "FORMAT C:". Sans ce message, nous risquons d'effacer tout le disque dur, ce qui peut être très fâcheux ! Par contre interdire l'effacement de façon systématique n'est pas une solution, car cette opération peut se révéler nécessaire.

Détecter des erreurs effectives ou potentielles nécessite une certaine préparation et la connaissance a priori des types d'erreurs généralement commises par les opérateurs. Nous allons examiner les conditions dans lesquelles sont commises les erreurs en notant que ce n'est pas l'erreur elle-même qui nous intéresse mais les circonstances qui ont favorisé son apparition.

L'analyse ne doit pas se contenter d'identifier les seuls événements ayant conduit à des erreurs humaines, événements que nous appelons événements d'Opérabilité (c'est l'opérateur qui est en cause). Il faut rajouter les événements dits de Sensibilité aux Perturbations et les événements dits de Manœuvrabilité que nous définirons plus loin. Sans la description de ces événements en effet, les erreurs commises peuvent ne pas être

compréhensibles (une erreur commise, par exemple mauvaise correction d'une assiette latérale anormale, en turbulence, n'a pas de sens si l'on n'a pas précisé la perturbation préalable.).

Revenons sur les notions d'incidents et d'accidents pour préciser le vocabulaire et quelques notions de base.

Pour généraliser nous appellerons Machine le Système que le ou les opérateurs doivent contrôler. Dans les cas que nous utiliserons principalement pour illustrer notre propos, la Machine est évidement l'avion.

On peut représenter l'état de fonctionnement de la machine à tout instant par un point, dit *point d'état*, dans un espace à n dimensions, chaque dimension étant attribuée à l'un des paramètres caractérisant l'état de la machine dans son ensemble, d'un système, d'un sous système ou d'un élément. Nous appellerons *espace d'état* l'espace dans lequel se déplace le point d'état. Ainsi les composants du point d'état d'un avion peuvent être l'incidence, la vitesse conventionnelle, le nombre de Mach, l'altitude, la longitude et la latitude de l'avion, paramètres caractérisant, entre autres, l'état de l'avion lui-même. Ce sont également les régimes de rotation des ensembles basse et haute pression des réacteurs, les températures devant turbines, la pression dans la bâche d'un circuit hydraulique, la pression cabine, la température dans le circuit de ventilation d'une génératrice, la tension d'alimentation d'un ordinateur, etc.

A chaque position du point d'état on peut faire correspondre une probabilité de catastrophe.

Au "milieu" du domaine, la probabilité de catastrophe est très faible. Elle n'est toutefois pas nulle car la liste des paramètres définissant le point d'état n'est pas complète. A titre d'exemple d'événement négligé dans la caractérisation de l'espace d'état, citons la chute d'un météore percutant la cabine. On peut trouver d'autres événements tout aussi "exotiques" qui sont négligés, à juste titre, lors de l'élaboration de l'espace d'état mais qui rendent la probabilité d'accident très faible mais non nulle (tremblement de terre endommageant la piste, tsunami envahissant la piste, éruption solaire détruisant l'électronique de bord, etc.). Mais l'on peut citer d'autres événements hautement improbables mais possibles comme la panne totale des trois circuits hydrauliques, la panne totale des moteurs, etc (ces événements très rares ont déjà été observés !).

Il existe par ailleurs des limites de l'espace d'état au-delà desquelles la probabilité de catastrophe est très voisine de l'unité. La notion de limite est floue, mais au voisinage d'une limite la probabilité de catastrophe varie plus ou moins rapidement d'une valeur proche de zéro à une valeur proche de l'unité. Il est toutefois commode de parler de limite en supposant que le franchissement d'une limite se traduit par un saut de probabilité de zéro (on assimile une probabilité très faible à une probabilité nulle) à un (on assimile une probabilité voisine de un à une certitude).

Fournissons quelques exemples.

- ⇨ L'incidence est limitée à une valeur maximale au-delà de laquelle se produit le décrochage aérodynamique, valeur qui dépend de la configuration avion et des conditions de vol (nombre de Mach en particulier).
- ⇨ La vitesse conventionnelle (pratiquement la vitesse lue sur l'anémomètre) est limitée à des valeurs maximales dépendant de la configuration de l'avion pour des raisons de résistance de la structure et à des valeurs minimales pour des raisons de Manœuvrabilité, entre autres.
- ⇨ L'altitude de l'avion est limitée inférieurement par des conditions de relief et supérieurement par des conditions d'aérodynamique (plafond de sustentation) et de confort des passagers (pressurisation).
- ⇨ Le régime de rotation des réacteurs est limité à une valeur maximale imposée par des raisons de tenue mécanique des ensembles tournants.
- ⇨ La pression dans un circuit hydraulique ne peut dépasser une valeur critique sans risques de rupture de canalisations ou de joints et doit rester au-dessus d'une autre valeur critique, sans quoi les vérins alimentés sont inefficaces.

Il faut, toutefois, garder à l'esprit cette notion de variation de probabilité de catastrophe au voisinage d'une limite. Cette notion de limite est commode mais il ne faut pas en déduire qu'à l'intérieur des limites l'accident est "impossible", donc la sécurité "absolue" et qu'en dehors l'accident est inévitable !

C'est l'approche de ces limites qui est signalée par les alarmes, tout en conservant une certaine marge pour permettre à l'opérateur de réagir à temps.

Pour les avions civils on définit un *domaine autorisé*, à l'intérieur duquel la probabilité d'accident est jugée suffisamment faible pour que l'accident y soit considéré comme hautement improbable, et un domaine dit

périphérique à l'intérieur duquel la probabilité d'accident est encore suffisamment faible, mais d'où l'opérateur doit faire sortir le point d'état pour le ramener dans le domaine autorisé. La probabilité d'accident est ainsi maintenue à une valeur raisonnable, compte tenu du faible temps pendant lequel le point d'état demeure dans le domaine périphérique. Cette représentation permet de tenir compte, en partie, de l'évolution de la probabilité d'accident au voisinage des limites, les alarmes se trouvant à la frontière entre le domaine autorisé et le domaine périphérique.

Nous dirons qu'il y a accident chaque fois qu'un paramètre d'état franchit une limite. Ceci constitue une schématisation de la réalité mais cette définition est commode.

Ainsi, assurer la sécurité revient à fournir à l'opérateur les moyens de maintenir le point d'état à l'intérieur des limites.

Bien entendu, cela signifie seulement que, dans ces conditions, la probabilité d'accident est estimée suffisamment faible pour que l'accident soit considéré comme raisonnablement improbable.

Comment se produit l'accident, c'est-à-dire le franchissement d'une limite ?

Les règles d'emploi du système imposent à l'opérateur de maintenir le point d'état à une valeur nominale ou dans un domaine suffisamment éloigné des limites. En général, le franchissement d'une limite est dû à une succession d'événements qui déplacent le point d'état. On notera qu'aucun des événements ne joue un rôle prépondérant. Aussi est-il vain de chercher à définir "la cause" d'un accident. Chaque événement joue un rôle dans le déplacement du point d'état et il suffit qu'un seul d'entre eux, peu importe lequel, n'ait pas lieu pour que l'accident soit évité.

Ainsi dans les accidents évités de justesse (le "near miss" des anglo-saxons), on remarque bien souvent qu'il eût suffi de la coïncidence d'un seul autre événement pour provoquer la catastrophe; mais cet événement n'en aurait pas été pour autant "la cause".

Nous retiendrons donc que nous appelons *incident* toute succession d'événements qui provoque le déplacement du point d'état et le rapproche d'une limite et qu'un *accident* est le résultat d'un franchissement de limite.

Ainsi un accident peut se décrire par une succession d'événements dont le dernier conduit au franchissement d'une limite amenant la probabilité de catastrophe, blessures ou perte de vies humaines, destructions de matériel, à une valeur inacceptable.

Un incident peut se décrire par une succession d'événements dont le dernier met le système dans une situation dangereuse puisque voisine d'une limite.

La distinction entre accident et incident est utile sur le plan de la justice ou de la gestion. Elle est sans intérêt pour le retour d'expérience en matière de sécurité. Il s'agit en effet de dégager les scénarios "accidentogènes", peu importe que leurs conclusions aient été plus ou moins catastrophiques. Un accident n'est qu'un incident qui a "mal tourné". Dans ce qui suit nous ne ferons donc plus la distinction entre accident et incident et les appellerons tous accidents.

Un déplacement du point d'état est provoqué par des événements de trois types et de trois types seulement.

- événements d'Opérabilité,

L'opérateur dispose des commandes nécessaires pour maintenir le point d'état dans le domaine autorisé, mais il laisse le point d'état se rapprocher d'une limite ou même la dépasser.

Les conditions favorisant l'apparition de ces événements sont la maladresse, la surcharge de travail, l'absence de stimuli se traduisant par une baisse de vigilance, l'erreur de représentation (mauvaise utilisation des données disponibles, refus a priori des données utiles, mauvaise estimation du risque, etc.). Nous avons déjà cité ces conditions découlant du comportement des opérateurs et y reviendrons ultérieurement.

Pour ce type d'événement, les performances du système et de ses moyens de contrôle ne sont pas en cause. On pourrait, théoriquement, pour chaque événement, concevoir un automatisme qui éviterait la dérive du point d'état. C'est l'opérateur et uniquement l'opérateur qui est en cause (compte tenu du système de présentation des données, du système de commandes et des procédures utilisées).

- événements de Sensibilité aux Perturbations,

Les perturbations qu'il y a lieu de considérer sont caractéristiques de la machine. Elles ne sont pas les mêmes pour un avion léger, un avion de transport, une centrale nucléaire ou une motrice de TGV.

Citons quelques exemples en matière d'aviation de transport civil.

Par Perturbation Interne, nous entendons essentiellement tout événement se traduisant par la perte d'une fonction assurée par l'un des systèmes (panne d'un réacteur, panne d'un régulateur, panne d'un transformateur dans un ensemble d'alimentation électrique, panne d'un ordinateur par exemples) ou par une avarie du matériel (rupture ou blocage d'un câble de commande, éclatement d'un pneumatique, rupture d'une canalisation hydraulique, ouverture d'une porte de soute, etc.).

Il faut bien noter que les événements de Sensibilité aux Perturbations Internes ne font intervenir que la réponse transitoire du système à l'apparition de la perturbation. Une fois la panne ou l'avarie établie, on se trouve en présence d'un nouveau système, ayant ses caractéristiques et ses performances propres, et qu'il convient d'étudier tel quel vis-à-vis des événements des trois types.

Ainsi la panne d'un régulateur peut se traduire par un changement brutal de la valeur de consigne et une réponse plus ou moins rapide du système régulé jusqu'à ce que l'opérateur, ou une sécurité, mette le régulateur défaillant hors service. Le transitoire ainsi provoqué déplace le point d'état dans l'espace d'état.

Une avarie peut avoir deux effets, le déplacement du point d'état (embardée latérale sur éclatement de pneumatique) ou la modification d'une limite (baisse de la vitesse maximale autorisée si la structure a été endommagée suite à une rupture).

La modification des paramètres de fonctionnement est indépendante du comportement de l'opérateur, elle ne dépend que des caractéristiques du système, de la nature et de l'amplitude de la perturbation. Dans certains cas, il serait possible de concevoir un automatisme réduisant la réponse transitoire, mais non l'éliminant. Il serait illusoire de compter sur l'opérateur pour faire ce travail.

- événements de Manœuvrabilité.

Pour suivre un programme donné, défini par l'objectif de l'opération (suivi d'une trajectoire donnée) ou pour ramener le point d'état à la valeur nominale (ou dans le domaine autorisé) à la suite d'un écart dû à des événements des deux premiers types, l'opérateur doit effectuer une "manœuvre" qui, en général, amène le point d'état à se déplacer et quelquefois à se rapprocher d'une limite. Ce déplacement constitue un événement de Manœuvrabilité.

Le déplacement du point d'état est imposé par la manœuvre à effectuer et les caractéristiques du système. Il ne dépend pas de l'habileté de l'opérateur. Même un automatisme infiniment performant ne peut l'éviter. Ces événements dépendent de la machine et du type de mission qui lui est confié.

Quelques exemples peuvent éclairer cet aspect fondamental de l'événement de Manœuvrabilité.

Pour éviter un obstacle, par exemple pour éviter une collision avec un autre avion, le pilote est amené à effectuer une manœuvre de mise en virage. Si la manœuvre d'évitement impose une incidence supérieure à l'incidence maximale autorisée, le pilote se trouve en présence de deux solutions aussi mauvaises l'une que l'autre. Ou bien il affiche une incidence supérieure à l'incidence maximale et l'avion décroche, ou bien il respecte la limitation et il ne peut éviter la collision. Ainsi, suite à une erreur d'Opérabilité (le pilote n'a pas détecté à temps l'autre avion parce que la visibilité était mauvaise par exemple), la Marge de Manœuvrabilité (rayon de virage minimal) était insuffisante pour faire face à la demande.

Un exemple analogue est celui du conducteur amené à effectuer à vitesse élevée un virage serré imposé par la route. Ou bien il affiche le braquage des roues nécessaire pour fournir la force latérale assurant le virage et il dépasse la limite d'adhérence des pneumatiques, ou bien il respecte cette limite et la voiture sort de la route parce que le rayon de virage est insuffisant.

De même, face à un obstacle le conducteur freine suffisamment, mais il dépasse la limite d'adhérence des pneumatiques et la force de freinage s'effondre, ou bien il respecte cette limite mais le freinage est insuffisant.

On notera qu'un système automatique interdisant de dépasser l'incidence maximale ou la limite d'adhérence ne permettrait pas d'éviter l'accident. C'est la marge de Manœuvrabilité disponible qui est insuffisante et aucun système ne peut l'augmenter.

Nous distinguons ainsi deux types d'événements de Manœuvrabilité :

- les événements de Manœuvrabilité de corrections d'écarts.

  L'opérateur doit effectuer une manœuvre pour ramener le point d'état à la valeur de consigne, à la suite d'un déplacement dû à un événement des deux autres types.

  Ainsi à la suite d'une erreur d'Opérabilité le pilote, en approche en turbulence, a laissé la vitesse diminuer et l'avion passer au-dessous de la trajectoire nominale. Le pilote tire sur le manche pour accroître l'incidence et pousse les manettes réacteurs. Au cours de l'opération de correction le point d'état se déplace (l'incidence se rapproche de la limite de décrochage) et ne suit pas nécessairement le trajet inverse du trajet initial dû à l'effet de la turbulence. Le trajet de retour est imposé par les caractéristiques du système et ne dépend pas de l'habileté de l'opérateur.

  Bien entendu peut se superposer à cet événement de Manœuvrabilité, un événement d'Opérabilité si l'opérateur effectue mal la manœuvre de correction ou ne l'effectue pas parce qu'il n'a pas noté le déplacement du point d'état. Mais il ne faut pas confondre ces deux types d'événements.

- les événements de Manœuvrabilité imposés par la mission.

  Par exemple, le contrôle au sol demande une mise en palier provisoire au cours d'une descente. Pendant l'opération de mise en palier, le point d'état se déplace et, bien qu'allant d'une position initiale à une position finale respectant toutes deux des marges raisonnables par rapport aux limites, il peut se rapprocher provisoirement d'une limite (ici la limite d'incidence maximale). Ainsi le rapprochement d'une limite ne dépend que des caractéristiques du système et non de l'habileté de l'opérateur. Là encore, peut se superposer à l'événement de Manœuvrabilité, un événement d'Opérabilité si l'opérateur effectue mal la manœuvre. Mais il ne faut pas confondre ces deux types d'événement.

Tous les changements de phases ou de sous phases (accélérations, virage, mise en palier etc.) imposent des manœuvres au cours desquelles le point d'état se déplace. C'est pourquoi les procédures imposent des points d'état de consigne, en prenant des marges suffisantes par rapport aux limites pour couvrir les manœuvres maximales raisonnablement prévisibles.

En conséquence, à la suite d'une série d'événements des trois types décrits, le point d'état se rapproche d'une limite de telle sorte qu'un dernier événement, toujours de l'un des trois types, conduit le point d'état à franchir une limite, provoquant l'accident.

L'étude des événements de Sensibilité aux Perturbations et des événements de Manœuvrabilité conduit à prendre des marges entre le point d'état et les limites de façon à pouvoir faire face aux perturbations maximales et aux manœuvres maximales raisonnablement probables.

Il est donc important dans l'analyse de retour d'expérience de bien identifier ces événements car, outre l'explication de l'apparition d'événements d'Opérabilité dans les manœuvres de corrections, ils peuvent mettre en évidence une insuffisance des marges entre point d'état et limites et conduire à modifier les consignes opérationnelles (par exemple, modification des vitesses d'approche recommandées en turbulence).

Ces événements sont résumés dans les grilles **GASP** (Grille d'Analyse des événements de Sensibilité aux Perturbations) et **GAME** (Grille d'Analyse des événements de Manœuvrabilité) présentées au chapitre 11 dans le cas particulier de l'analyse des incidents et accidents d'avions de transport civils.

Un retour sur la notion de limite et de domaine autorisé est nécessaire avant de poursuivre plus avant.

Les limites que nous avons décrites jusqu'ici sont les valeurs des paramètres au-delà ou en deçà desquelles la probabilité de catastrophe est voisine de l'unité. Nous appellerons ces limites "limites absolues", tout en reconnaissant leur caractère un peu flou; en toute rigueur il faudrait définir les limites absolues avec une probabilité de catastrophe associée, 10^{-3} / heure par exemple; on voit tout de suite l'aspect purement théorique de cette définition.

En pratique, on ne laisse pas à l'opérateur le loisir de laisser volontairement son système frôler les limites absolues. On lui fixe des "limites opérationnelles", correspondant à une probabilité raisonnablement faible de catastrophe pour fournir des marges vis-à-vis des différents aléas. Si l'on vise une probabilité globale d'accident de l'ordre de 10^{-7} / heure, on se fixe généralement la limite opérationnelle à cette valeur (là encore cette précision est toute théorique, mais l'ordre de grandeur doit être retenu).

On définit ainsi un domaine opérationnel, à l'intérieur duquel la probabilité de catastrophe est raisonnablement faible, entouré d'un domaine dit "périphérique" au sein duquel la probabilité de catastrophe varie de 10^{-7} / heure à 10^{-3} / heure.

L'opérateur a pour consigne de maintenir le point d'état à l'intérieur du domaine opérationnel. Si pour une raison quelconque le point d'état sort du domaine opérationnel pour pénétrer dans le domaine périphérique, l'opérateur a la consigne impérative de ramener le plus rapidement possible le point d'état dans le domaine opérationnel (certains automatismes sont conçus pour exercer cette fonction).

Le point nominal d'état n'est pas en général sur la limite du domaine opérationnel. On le choisit en prenant des marges vis-à-vis des limites opérationnelles pour couvrir les événements d'Opérabilité, de Manœuvrabilité et de Sensibilité aux Perturbations et ne pas imposer à l'opérateur une surveillance permanente du point d'état.

On voit donc apparaître deux types de marges, les marges opérationnelles entre le point d'état nominal et les limites opérationnelles, les marges de sécurité entre les limites opérationnelles et les limites absolues.

Ainsi en configuration d'approche, train et volets sortis, la Vitesse Maximale Autorisée n'est pas la vitesse où pourraient apparaître des ruptures de structure, mais une vitesse inférieure (marges pour les évolutions et les rafales). On remarquera, en outre, que le franchissement de cette vitesse ne conduit pas à la catastrophe (on en est encore loin), mais impose une réduction immédiate de vitesse au pilote. Un tel franchissement doit être considéré comme un incident, d'autant plus grave que la pénétration dans le domaine périphérique a été profonde et durable, mais ne constitue pas un accident. Par contre, si la vitesse de rupture est franchie, on peut admettre que la limite absolue a été violée.

L'étude des événements d'Opérabilité conduit à des recommandations très différentes de celle des deux autres types d'événements. Elle a pour objet la prévention des erreurs des opérateurs. C'est le domaine des facteurs humains qui nous intéresse ici plus particulièrement.

Détecter des erreurs effectives ou potentielles nécessite une certaine préparation et la connaissance a priori des types d'erreurs généralement commises par les opérateurs. Examinons les conditions dans lesquelles sont commises les erreurs en notant que ce n'est pas l'erreur elle-même qui nous intéresse, mais les circonstances qui ont favorisé son apparition.

Généralement une erreur est commise dans cinq circonstances :

- ⇨ **l'opérateur est débordé par la charge de travail imposée par la tâche**. Il n'exécute pas l'action appropriée au bon moment, ou bien il ne prend pas la bonne décision parce qu'il n'a pas le temps d'analyser les données dont il dispose, ou bien il ne prélève pas une donnée utile, ou bien il ne transmet pas une donnée importante.

  A titre d'exemple tiré de la vie quotidienne, citons le conducteur arrivant à un carrefour et devant lire un grand panneau lui indiquant toutes les directions possibles (sauf celle qui l'intéresse). Surchargé par la lecture et le travail d'identification des villes précédant ou suivant sa destination, il ne surveille pas la route et ne perçoit que trop tard le véhicule qui a ralenti devant lui pour les mêmes raisons de surcharge de travail. Ne parlons pas du cas, réel, vu aux environs de Lille, où le panneau indique "Toutes directions" à droite et "Autres directions" à gauche, ce qui impose une charge de travail intense de décision !

- ⇨ **le système ne fournit aucun stimulus à l'opérateur parce que tout est stable**. Dans ces conditions l'attention de l'opérateur est réduite et il rate une action, ne relève pas un changement d'état, oublie de prendre une décision ou de transmettre une information.

Ces deux situations, charge de travail trop élevée ou manque de stimuli, dépendent de l'état physiologique et psychosociologique de l'opérateur. La charge de travail peut être trop forte ou l'attention peut être trop réduite pour un opérateur travaillant à deux heures du matin, fatigué, grippé, anxieux ou préoccupé, alors que la charge ou l'attention est normale pour un opérateur reposé, en début de mission, sain et sans souci.

⇨ **l'opérateur commet un geste maladroit**, prononce un mot à la place d'un autre, entend "de travers" un message, lit une valeur erronée sur un indicateur parce qu'il est mal éclairé, etc. Toutes ces erreurs sont regroupées sous le nom de **lapsus** (gestuel, verbal, auditif, etc.) ou de **maladresses**.

A titre d'exemples, l'opérateur accroche une commande avec sa manche en cherchant à en atteindre une autre. L'opérateur demande une manœuvre "à droite" en pensant "à gauche" (qui n'a pas commis cette erreur en guidant un conducteur en ville sur un trajet difficile !).

Ou bien encore, l'opérateur renverse sa tasse de café sur un pupitre électronique provoquant un court-circuit fatal ou déclenche une commande en posant sa documentation sur une touche sensible, etc.

Il faut noter que bien souvent une erreur de conception de matériel facilite ce genre d'erreur (il faut prévoir un porte gobelet et une tablette pour la documentation par exemple).

⇨ **Conscience Erronée de la Situation.**

Il y a cinq types de Conscience Erronée de la Situation

a/ **Une Image Présente, Externe ou Interne, est erronée** ce qui conduit à une mauvaise décision d'action ou à une mauvaise estimation de l'Image Future.

Par exemple, le pilote pense qu'il a déjà dépassé la colline dans l'axe de la piste alors que cette colline est encore devant et il commence sa descente trop tôt.

Le contrôleur pense, à tort, qu'il n'y a pas de trafic sur la piste en service et il donne l'autorisation d'atterrir sur cette piste.

b/ **Une Image Future, Externe ou Interne, est erronée** ce qui conduit à une mauvaise décision d'action.

Par exemple, le pilote pense que les performances de l'avion sont suffisantes pour monter rapidement et éviter le sommet de la colline.

Le contrôleur pense que son ordre de décollage va être immédiatement suivi d'effet et qu'en conséquence la piste sera rapidement disponible pour un atterrissage.

c/ Utilisation d'un **mauvais Modèle de Tâche** conduisant à une mauvaise Image désirée.

Une mauvaise définition des responsabilités de l'équipage ou une mauvaise définition de la répartition des tâches entre les membres de l'équipage ou entre l'équipage et le contrôleur peuvent conduire à des erreurs sur le choix du Modèle de Tâche et par la même à une erreur sur une Image Désirée.

d/ Utilisation d'une **Image "a priori"**

L'opérateur ayant exécuté ou croyant avoir exécuté une séquence d'actions décidées au temps T_1, bâtit au temps T_2 une Image Présente identique à l'Image Future qu'il avait prévue au temps T_1 ou qu'il avait bâtie à la suite d'observation d'événements entre les temps T_1 et T_2. Il ne vérifie pas l'exactitude de cette Image ou ne vérifie que les paramètres qui confirment cette prédiction.

e/ Utilisation d'un mauvais **Modèle de Risque**

L'opérateur a en tête des Images Présentes et Futures exactes, mais il n'évalue pas correctement le risque associé à ces situations.

Ces erreurs sont résumées dans la grille dite **GAFE** (Grille d'Analyse des Facteurs d'Erreurs), dont l'origine lointaine est la grille utilisée au cours de l'opération RACHEL (voir chapitre 8) et plus récemment la grille GAFH (Grille d'Analyse des incidents sous l'aspect Facteur Humain) mise au point avec la Marine Nationale et la société Technicatome pour le retour d'expérience sur les sous-marins nucléaires.

Toutes ces erreurs ont des causes premières qu'il convient d'identifier pour les combattre. Ce n'est pas en effet l'erreur finale qu'il convient d'éliminer. Cette dernière est la conséquence quasi inévitable, sauf coup de chance, de circonstances préalables que seule une analyse fine des événements permet de reconnaître. Il arrive aussi que l'erreur une fois commise n'ait pas de conséquences graves (entamer la descente finale deux minutes trop tôt dans la région parisienne n'a pas les mêmes conséquences que dans la région grenobloise !). Il n'en reste pas moins que cette erreur a été commise et qu'il est important d'analyser les circonstances qui l'ont générée. En effet, répétons-le, les mêmes causes ayant les mêmes effets, tout porte à croire que ce type d'erreur se reproduira et que l'on n'aura pas toujours la chance qu'elle soit commise dans des conditions telles que les conséquences n'en soient pas catastrophiques.

Ainsi nous ne saurions trop insister sur la nécessité du retour d'expérience et l'analyse des incidents en service, chacun exposant franchement les erreurs commises en détaillant soigneusement les circonstances préalables. Il ne sert à rien de signaler une erreur d'affichage de fréquence de balise si l'on ne précise pas la succession des opérations, des manœuvres, des décisions, des échanges d'informations qui ont précédé l'erreur. Il ne s'agit pas de s'indigner devant l'erreur commise et de sanctionner, mais de comprendre l'enchaînement des faits pour éviter que cet enchaînement ne se reproduise trop fréquemment.

Le Retour d'Expérience ce n'est ni Accuser, ni Excuser mais Expliquer.

Cette démarche est fondamentale. On ne peut prévoir tous les cas possibles et qui pourra prendre les mesures nécessaires pour limiter les erreurs si celles-ci sont soigneusement dissimulées ?

Les incidents décrits dans les fiches de RETOUR D'EXPERIENCE doivent être présentés, nous venons de le voir, sous forme de chaînes d'événements de trois types

- les événements d'Opérabilité mettant en cause les caractéristiques de l'opérateur humain,
- les événements de Sensibilité aux perturbations externes et internes,
- les événements de Manœuvrabilité caractérisant les manœuvres imposées par l'objectif de la tâche ou les manœuvres de corrections d'écarts.

La description des événements eux-mêmes, doit être précédée d'une description des conditions générales dans lesquelles se sont déroulés ces événements (conditions physiques telles que température, éclairage, visibilité, etc., conditions physiologiques, psychologiques et sociologiques des opérateurs.).

La connaissance de ces conditions est utile à deux titres :

- D'une part elles peuvent influer sur l'apparition des erreurs. Ainsi des températures extrêmes, une ambiance sonore intense, la fatigue, les soucis personnels, etc. réduisent les capacités des opérateurs et favorisent les erreurs, sans en être pour autant la cause directe. Elles agissent en tant qu'**Amplificateurs du Risque d'Erreur**. Leur connaissance permet donc d'expliquer l'apparition d'erreurs aux cours d'événements d'opérabilité.

  Très souvent la fatigue est citée comme cause d'une catastrophe. C'est le plus souvent une mauvaise analyse. En effet la fatigue ne fait que favoriser l'apparition d'une erreur, mais encore faut-il que cette erreur soit potentielle. Fatigué ou non, si l'opérateur n'est pas dans une situation où une erreur est possible, il n'en commettra pas ! Seuls quelques cas de conditions physiologiques extrêmes peuvent être cause directe de catastrophe (évanouissement, malaise incapacitant, mort subite, aveuglement par une lumière intense, etc.) parce qu'ils rendent impossible la conduite de la machine.

- Leur connaissance permet d'autre part d'estimer la probabilité de retrouver des conditions analogues en service et donc permet de juger l'utilité de trouver un remède pour limiter la probabilité d'apparition d'incidents du même type. Si ces conditions se révèlent exceptionnelles on peut estimer qu'il n'est pas nécessaire de pousser l'analyse de l'incident jusqu'à la recherche de remèdes.

La GARE (Grille des facteurs Amplificateurs du Risque d'Erreur) **dresse la liste des principales conditions générales dans lesquelles se sont déroulés les événements.** (voir chapitre 11)

Une fois reconnus les événements d'opérabilité caractérisés par la **GAFE**, il nous reste à identifier les causes premières des cinq Facteurs d'Erreurs que nous venons de citer et les causes de la plupart des Facteurs d'amplificateurs de gravité. Ces causes premières se répartissent en cinq groupes de défauts de conception du système.

Le RADOS (Répertoire d'Analyse des Défauts Opérationnels Système) est destiné à identifier le Défaut du Système ayant contribué à l'apparition de chaque événement d'Opérabilité.

⇨ les **Défauts d'Organisation**

Ces défauts se divisent eux-mêmes en quatre catégories :

⇨ *les opérateurs ne savent pas ce qui est de leur responsabilité*, ce qu'ils doivent faire eux-mêmes, ce qu'ils ne doivent pas faire, ce qu'ils peuvent déléguer, quelles informations ils doivent transmettre et à qui. Autrement dit la répartition des taches entre les divers opérateurs est mal définie, du moins dans l'esprit des opérateurs. En conséquence ils omettent une opération croyant qu'elle n'est pas de leur ressort ou exécutent une action normalement impartie à un autre opérateur. Ce type d'erreur est bien souvent à l'origine d'une erreur de représentation pour un autre opérateur.

A titre d'exemple la responsabilité de l'anticollision avec le relief est du ressort du contrôle au sol ou de l'équipage suivant les phases de vol, ce qui peut engendrer une certaine confusion.

Ce type de défaut correspond à la question "*Qui doit faire ?*".

⇨ *les définitions des objectifs, des contraintes, des marges disponibles comportent des erreurs ou des oublis,* ce que nous regroupons sous le terme de Tâches mal définies.

Dans certains cas, les situations nominales recommandées sont trop près des limites ce qui laisse des marges trop faibles pour couvrir les aléas (erreur d'Opérabilité, Perturbations, Manœuvres).

Il arrive aussi bien souvent que les opérateurs s'imposent eux-mêmes des contraintes inutiles, par exemple mettent en priorité la régularité avant la sécurité ("faire l'heure" pour la SNCF, atterrir immédiatement même dans des conditions limite pour un pilote de transport).
Ce type de défaut correspond à la question "*Que doit-on faire ?*".

⇨ *les opérateurs ne savent pas comment exécuter leur tâche* ou encore les procédures qu'on leur impose sont mal adaptées aux caractéristiques de l'opérateur humain et aux moyens dont ils disposent en homme et matériel.

Cette situation a des origines multiples,
- procédures matériellement défectueuses (erreurs de frappe, photocopie imparfaite, etc.),
- procédures imparfaites parce que mal rédigées, complexes, non expliquées, rédigées en termes juridiques et non en termes techniques ou opérationnels,
- procédures trop générales laissant l'opérateur devant un choix difficile à faire,
- procédures imposant des charges de travail ponctuelles trop élevées ou imposant des tâches fastidieuses (longs temps d'attente entre opérations, attente d'un événement qui ne se produit que très rarement, surveillance sans événements notoires) néfastes à la vigilance (attention il ne s'agit pas de charger les opérateurs par des opérations artificielles ou inutiles !), etc.

A titre d'exemple de procédure mal conçue citons le cas où une vérification est demandée et où rien n'est prévu si la vérification est négative. "Vérifiez, au bout de dix minutes de chauffage, que le four est à 150°" et rien n'est prescrit si la température relevée est 140° !

Quelquefois les procédures sont rédigées par des juristes dans le but, non avoué, de faire porter toute la responsabilité sur les opérateurs en cas d'erreur. Cela se traduit par des consignes du style "Il n'est pas interdit de ne pas ouvrir le robinet tant que le réservoir n'est pas plein.". Nous n'avons rien inventé; des pages entières du règlement d'une grande compagnie de transport terrestre étaient rédigées sur ce principe (cette situation s'est heureusement améliorée depuis quelque temps !).

Cela se traduit le plus souvent par des opérations ratées, à l'origine d'erreurs de représentation pour l'opérateur lui-même ou pour un autre opérateur qui pense que la tâche de son collègue a été correctement exécutée.
Ce type de défaut correspond à la question "*Comment faire ?*".

⇨ *les opérateurs ne disposent pas de moyens suffisants,* en personnel ou en matériel pour exécuter leur tâche. Cela conduit en général à des surcharges de travail, quelque fois de courte durée, mais suffisantes pour conduire à l'erreur. Ce cas se rencontre souvent dans les postes de travail à charge moyenne faible ne justifiant pas un nombre d'opérateurs suffisant pour faire face aux pointes ou dans le cas de procédures prévoyant des transmissions de données alors que les moyens de transmission ne sont pas disponibles (centre de contrôle fermé la nuit par exemple).
Ce type de défaut correspond à la question "*Avec qui et quoi peut-on faire ?*".

⇨ les **défauts de Conception de la Machine**.

Le matériel n'a pas été conçu en tenant compte des caractéristiques physiques, physiologiques et psychologiques des opérateurs, ou encore la conception repose sur des principes pouvant conduire, dans des cas rares mais possibles, à des situations dangereuses.

Ces défauts sont à l'origine d'une saisie erronée de données ou d'une erreur d'action sur une commande conduisant à une erreur de représentation. A titre d'exemples citons les touches d'ordinateur trop petites et trop rapprochées (problème de désignation en turbulence), les messages comportant des signes tels que *, # ou & ayant des significations différentes d'un message à l'autre, les codes de couleurs reposant sur plusieurs philosophies, etc..

Citons les commandes de ponts roulants constituées d'un boîtier comportant six touches alignées indiquées L (pour Left, gauche), R (pour Right, droite), FW (pour Forwards, vers l'avant), BW (pour Backwards, vers l'arrière), U (pour Up, haut), D (pour Down, bas), alors que le boîtier peut être orienté n'importe comment par rapport à la charge ce qui fait perdre toute signification aux notions de gauche, droite, avant et arrière. Citons encore le cas où la touche Up est située au dessous de la touche Down ! (Là encore, nous n'avons pas inventé ces exemples !).

Nous avons donné de nombreux exemples de ce type de défaut d'interface dans les chapitres 3 et 4.

Les interfaces sont les pupitres d'instruments, les pupitres de commandes, les transparents isolant le poste de pilotage du monde extérieur, les moyens d'observation de l'environnement, les moyens de communication entre les opérateurs, les textes de consignes et de procédures.

Ces défauts peuvent être divisés en trois groupes, illustrés par quelques exemples :

⇨ *mauvaise conception de base*.

- Structure conçue en négligeant un processus de rupture possible (cas du Comet pour lequel le dessin des hublots conduisait à une concentration de contraintes, acceptables en efforts statiques mais inadmissibles en contraintes alternées, phénomène dit de "fatigue" mal connu à l'époque).
- Automatisme dont la logique peut conduire, dans certains cas, à une situation dangereuse (cas de certains pilotes automatiques, équipant les avions de l'avant dernière génération, dont un mode de base, maintien de la vitesse verticale, conduisait, à haute altitude, à une réduction de la vitesse aérodynamique allant, sans protection, jusqu'au décrochage et la perte de contrôle. Voir l'accident du DC10 d'Aeromexico décrit au chapitre 7).
- Le principe de l'automatisme interdisant la sortie des destructeurs de portance tant que les deux amortisseurs de train ne sont pas enfoncés (ce qui évite la manœuvre dangereuse d'ouverture en vol) a conduit à l'accident de Varsovie déjà cité au chapitre 2.
- Siège éjectable de la première génération à commandes entièrement manuelles pour le largage de la verrière, la commande d'éjection, la séparation du siège et du pilote, l'ouverture du parachute (l'accélération brutale à l'éjection conduisait la plupart du temps à l'évanouissement du pilote qui se trouvait quelque peu handicapé pour effectuer manuellement les deux dernières manœuvres vitales, séparation du siège et ouverture du parachute !).

⇨ *mauvaise conception de l'interface sur le plan ergonomie mécanique*.

Eclairage, chauffage, ventilation, sièges, dispositions et tailles des afficheurs, dispositions, tailles, formes et débattements des commandes, dispositions, formes, tailles, couleurs et caractères des étiquettes, etc. La conception ne tient pas compte des capacités mécaniques et physiologiques, de la taille et de la forme des membres de l'opérateur humain.

⇨ *mauvaise conception de l'interface sur le plan ergonomie mentale*.

Echelles, zéros des afficheurs, sens d'action des commandes, synoptiques, schémas sur écran, etc. Nous renvoyons aux nombreux exemples donnés dans les chapitres 2 et 3.

⇨ les **défauts de Conception de la Formation**

Ces défauts peuvent être divisés en deux groupes :

⇨ *mauvaise conception de la formation de base*

- méconnaissances dans les domaines élémentaires de la lecture, de l'écriture, des calculs mentaux, de l'arithmétique, des langues parlées, etc.;
- méconnaissances dans le domaine des techniques, mécanique, physique, électricité, électronique, informatique, aérodynamique, hydraulique, résistance des structures, usinage, soudage, langue technique, etc.
- méconnaissance des règles générales de transmission de l'information, méconnaissance des règles de sécurité, méconnaissances dans le domaine du comportement de l'homme face à la machine, etc.

⇨ *mauvaise conception de la formation spécifique au système*

- méconnaissance
  des modèles de fonctionnement du système conduisant à des erreurs de décisions,
  des modèles utilisés pour la captation des données,
  des modèles utilisés pour l'action sur les commandes,
  de l'organisation en cours (répartition des tâches),
  des procédures,
  de l'organisation générale de l'entreprise et de ses objectifs,
- manque d'entraînement ou mauvaises méthodes d'entraînement,
- mauvaise mise à jour des connaissances (formation continue).

⇨ les **Défauts de conception ou de réalisation de la Documentation,**
les **Informations erronées, non transmises ou matériellement mal transmises** aux utilisateurs,

La documentation comprend la documentation technique relative aux matériels, les documents de navigation (cartes et documents terrains), les documents administratifs, etc.

Les informations, qui constituent une documentation provisoire, concernent les modifications de matériels, de procédures, d'organisation, les incidents ou accidents identifiés, etc.

⇨ *Défauts matériels*

Documentation inexistante, mal présentée matériellement (photocopie défectueuse, taille ou volume incompatible avec une utilisation dans le poste, etc.). Nous avons ainsi vu des plans d'installations à consulter sur le terrain par tous les temps, pluvieux ou venteux, constitués d'une feuille de six mètres sur deux !

Information non transmise (erreur de transmission, liste de destinataires incomplète ou erronée), mal présentée matériellement ou mal transmise (Fax défectueux, incomplet, etc.).

⇨ *Contenu erroné*

Les données fournies par la documentation conduisent à des erreurs quant aux modèles utilisés pour la saisie des données, les décisions, la transmission des informations et les actions sur les commandes.

La documentation est rédigée par les concepteurs et n'est pas adaptée aux besoins de l'utilisateur qui n'y trouve pas ce qu'il y cherche. Citons par exemple un manuel de vol d'un avion de ligne, où il est nécessaire de consulter cinq chapitres différents pour identifier les symboles figurant sur la planche affichée sur écran cathodique pour surveillance du train d'atterrissage (chapitre Train, chapitre Commandes de Vol, chapitre Frein, chapitre Pneumatiques, chapitre Commandes de roulage).

Nous avons vu des cartes d'approche de terrains contenant des erreurs sur des relèvements de balises ou indiquant des fréquences fausses. Sur l'une de ces cartes figurait la mention "Attention le GPWS peut retentir au cours de l'approche". Rappelons que le GPWS (Ground Proximity Warning System) signale une altitude trop faible par rapport au relief. La moitié des pilotes consultés sur la signification de ce message a déclaré "cela signifie que l'on ne doit pas tenir compte de cette alarme" et l'autre moitié a déclaré "il faut impérativement remettre les gaz". Le moins que l'on puisse dire est que cette indication est fâcheusement ambiguë. Nous ne savons d'ailleurs toujours pas quelle en est la signification réelle.

A titre d'exemple vécu, nous reproduisons, sur les pages suivantes, deux cartes d'approche à vue de la base d'Hyères. Nous laissons au lecteur le soin d'y détecter l'erreur. On imaginera sans peine la confusion mentale du pilote faisant une approche à vue du terrain en se repérant sur la carte fausse !

Les informations fournies contiennent des erreurs (codes de référence incomplets ou contenant des fautes de frappes, schémas faux, incomplets ou périmés, etc.).

Quelquefois les opérateurs utilisent une documentation "sauvage" (carnet personnel dont le contenu est incontrôlable).

⇨ les **Défauts Réglementaires**.

Pour assurer la sécurité, la puissance publique impose, par la loi, un certain nombre de règles que les concepteurs et les utilisateurs se doivent de respecter sous peine de sanctions.

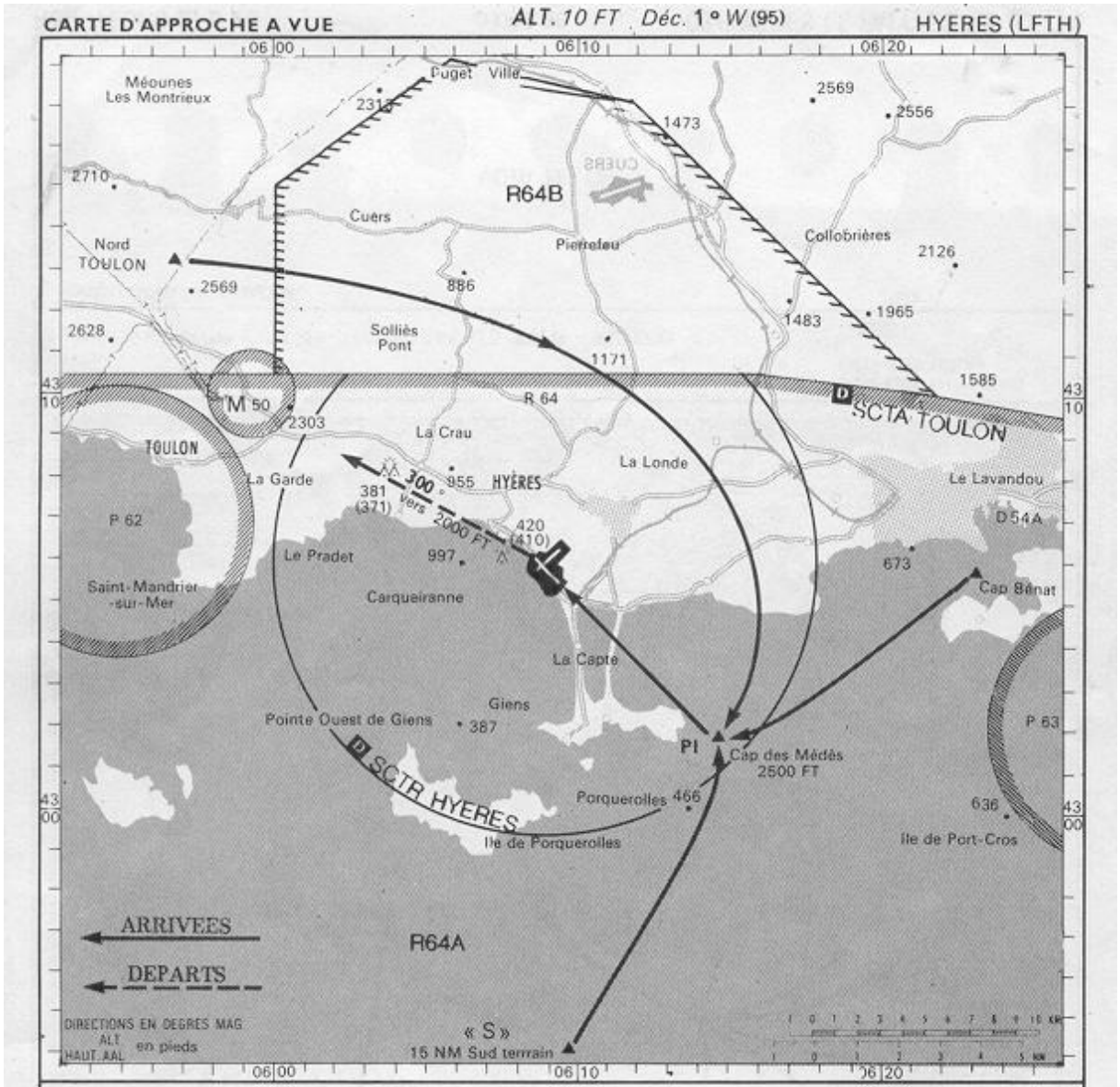
Or il arrive que ces règles deviennent caduques parce que les techniques ou les conditions d'emploi ont évolué. Les appliquer aveuglément peut conduire à un défaut système appartenant à l'une des quatre catégories que nous venons de définir.

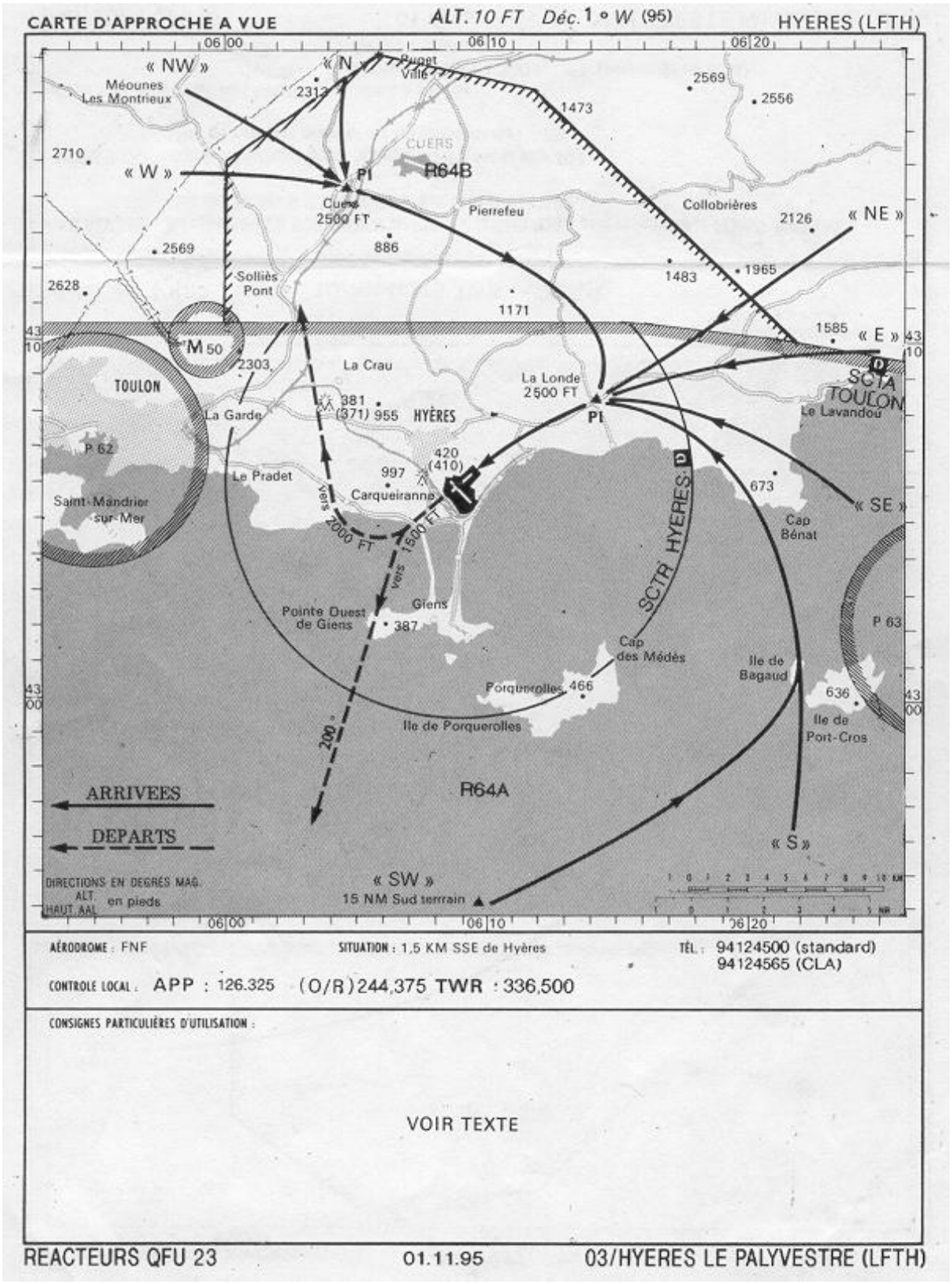
Le problème des défauts de réglementation est suffisamment vaste pour que nous y consacrions un chapitre entier (voir chapitre 10).

* * * * *

Les défauts systèmes, que nous venons de décrire, sont résumés dans la grille RADOS qui dérive en partie de la grille GAFH utilisée pour le retour d'expérience sur les sous-marins nucléaires.

Vous trouverez pages suivantes un exemple étonnant de documentation erronée pouvant conduire à la catastrophe.


CARTE D'APPROCHE A VUE
ALT. 10 FT Déc. 1° W (95)
HYERES (LFTH)
Méounes Les Montrieux
Puget Ville
2569
2556
1473
2710
R64B
Cuers
Pierrefeu
Collobrières
2126
Nord TOULON
2569
886
1483
1965
2628
Solliès Pont
1171
1585
M 50
2303
R 64
SCTA TOULON
La Crau
TOULON
La Garde
La Londe
Le Lavandou
955 HYERES
381 (371)
300°
vers 2000 FT
420 (410)
P 62
Le Pradet
997
673
D 54A
Saint-Mandrier -sur-Mer
Carqueiranne
Cap Bénat
La Capte
Giens
Pointe Ouest de Giens
387
P 63
PI
Cap des Médès 2500 FT
SCTR HYERES
Porquerolles
466
636
Ile de Porquerolles
Ile de Port-Cros
ARRIVEES
DEPARTS
R64A
DIRECTIONS EN DEGRES MAG
ALT HAUT. AAL en pieds
« S »
15 NM Sud terrain
AÉRODROME : FNF
SITUATION : 1,5 KM SSE de Hyères
TÉL. : 94124500 (standard) 94124565 (CLA)
CONTROLE LOCAL : APP : 126.325 (O/R)244.375 TWR : 336.500
CONSIGNES PARTICULIERES D'UTILISATION :
ARRIVEES : Se reporter à 2 500 ft QFE au POINT D'ENTREE, puis rejoindre le POINT INITIAL : Cap des Médès à 2 500 ft QFE aux ordres de l'APP.
DEPARTS : Après décollage, prendre impérativement le cap 300. Mise de cap vers mission sur instructions de l'APP.
CIRCUIT D'ATTERRISSAGE : Circuit à gauche.
- Altitude break : 1 500 ft QFE (avions de combat).
- QFU 14 : interdit.
REACTEURS QFU 32
01.11.95
02/HYERES LE PALYVESTRE (LFTH)



Pour compléter la confusion du pilote, les deux cartes ne se trouvaient pas côte à côte, mais sur deux pages recto-verso, ce qui en interdisait la comparaison.

Pour le lecteur intrigué, nous lui conseillons de noter comment est écrit le nom de la base militaire de Cuers sur l'une et l'autre carte. C'est là que réside le mode de détection, bien caché, de l'erreur !

Cinq remarques s'imposent enfin.

⇨ Il n'y a pas de correspondance biunivoque entre un Facteur d'Erreur de la GAFE ou un Facteur d'Amplification de Risque d'Erreur et un Défaut Opérationnel Système, tout au plus des corrélations fortes. Ainsi les maladresses ont très souvent pour origine une mauvaise conception du poste sous l'aspect ergonomie mécanique. Les erreurs de représentation par mauvaise utilisation de l'information sont souvent dues à un défaut de conception du poste sous l'aspect ergonomie mentale, mais elles peuvent provenir d'un défaut d'organisation (mauvaise répartition des tâches), etc.

⇨ L'utilisation des grilles GAFE, RADOS, GASP, GAME et GARE exige un complément d'information qu'il est hors de propos de développer ici, pour préciser, par des exemples, les types d'erreurs et de défauts trop sommairement décrits dans les lignes qui précèdent (voir le chapitre 12).

⇨ L'analyse des incidents et accidents est un travail de spécialiste. Il est hors de question de demander au rapporteur de faire lui-même cette analyse et de proposer des remèdes. C'est la confrontation des analyses de plusieurs incidents qui peut mettre en lumière un défaut système, permettre une évaluation des risques qu'il entraîne et guider l'analyste vers une proposition de remède. Il est donc nécessaire de mettre sur pied une organisation de retour d'expérience chargée de collecter les incidents et de les analyser, et de proposer des voies de recherche aux organismes compétents pour trouver des remèdes. Les analystes ne doivent pas être des ingénieurs débutants, mais d'anciens opérateurs (pilote de ligne en début de retraite par exemple pour les accidents aériens) connaissant bien les conditions réelles d'utilisation des matériels.

⇨ L'analyste doit faire deux hypothèses fondamentales avant de commencer une analyse, à savoir :

- l'opérateur est discipliné et n'a pas enfreint volontairement les règles de sécurité,
- les faits rapportés ont été fidèlement décrits.

Ce n'est qu'avec des arguments solidement étayés que l'analyste peut conclure, en fin d'étude, que l'opérateur a transgressé une règle de sécurité volontairement et non par suite d'erreurs ou que les faits rapportés sont faux.

⇨ Nous nous sommes axés sur la prévention des accidents dus aux erreurs de l'équipage. Autrement dit nous avons défini un type d'événement redouté, la perte de vies humaines pour les personnes transportées et les personnes survolées et un type "d'agression", l'erreur des équipages. Nous y avons subrepticement ajouté d'autres types d'agression, les agressions internes (pannes), les agressions atmosphériques (rafales, cisaillements de vent, givre, etc.), les agressions par les obstacles (relief, oiseaux, autres avions) et les agressions par l'action intempestive des passagers. Une étude de sécurité complète du système de transport aérien ne devrait pas se contenter de ces seuls types d'événements redoutés et d'agressions. Ce sont les plus importants, mais bien d'autres études relevant du retour d'expérience pourraient être menées dans le même esprit. Nous donnons en Annexe 1 une liste non exhaustive d'événements redoutés et d'agressions qu'il pourrait être intéressant d'étudier pour compléter une étude de sécurité du transport aérien ou pour toute étude de sécurité industrielle. Il est à noter que bien des incompréhensions en matière de retour d'expérience viennent du fait que les objectifs de chacun (types d'événements redoutés et types d'agressions) ne sont pas toujours clairement précisés. Il est évident que l'étude des détériorations ou du vol de matériel de cabine passager par vandalisme, l'étude des pertes d'exploitation par défaut de fourniture de carburant dans certaines contrées éloignées ou les effets du terrorisme peuvent relever des mêmes techniques de retour d'expérience mais exigent une organisation et des experts différents pour mener à bien l'analyse.

Le chapitre 11 est consacré à l'application pratique des méthodes d'analyse reposant sur l'utilisation des grilles **GAFE, RADOS, GARE, GAME** et **GASP**.

CHAPITRE 10

Le règlement, c'est le règlement !

Adjudant Flick

LES DÉFAUTS DE RÈGLEMENTATION

Dans le domaine du transport aérien, l'État, en vertu de conventions internationales (Conventions de Varsovie et de Chicago, ayant entre autres actions, créé l'Organisation de l'Aviation Civile Internationale) impose aux constructeurs un Règlement dit de Navigabilité que doivent respecter les aéronefs destinés au transport de passagers. L'État vérifie, par des essais, entre autres moyens, que les nouveaux avions satisfont ces règles et sanctionne un résultat correct par la délivrance d'un Certificat de Navigabilité. D'autres règles sont imposées pour vérifier la conformité des avions de série à la définition des premiers avions utilisés pour les essais de certification. Enfin, un règlement est destiné à vérifier que les compagnies aériennes utilisatrices ont mis en place les moyens et les procédures nécessaires à l'assurance d'une sécurité raisonnable.

Ce type de règlement se retrouve dans tous les domaines des industries de production ou des transports. La directive Sévéso en est un exemple dans le domaine des industries de production fabricant des matériaux intermédiaires dangereux.

Dans d'autres domaines, l'administration peut imposer des règles qui n'ont pas un objectif de sécurité mais des objectifs très différents, par exemple assurer la régularité des opérations financières et comptables.

Il arrive qu'une règle, judicieuse à une époque devienne caduque ou même néfaste à une autre époque, compte tenu des évolutions de la technique ou des méthodes d'exploitation. Dans d'autres cas deux règles, rédigées par des organismes différents et destinées à traiter des événements redoutés différents face à des types d'agression différents peuvent se révéler contradictoires au moment de leur application.

Les défauts décrits au chapitre précédent ont donné lieu à de nombreux développements dans les premiers chapitres. Nous nous sommes donc contentés de les citer rapidement. Par contre, les Défauts d'origine réglementaire ont un caractère spécifique et nouveau. Il est donc nécessaire de leur consacrer quelques pages particulières.

Très souvent les Défauts dits Réglementaires ont pour origine une méthode défectueuse d'élaboration des règles.

Il est très commode d'énoncer une règle de sécurité en imposant un moyen et c'est cette méthode qui est utilisée dans de nombreux règlements. Elle a l'avantage de faciliter la rédaction et la vérification de la règle. Le moyen est décrit en termes techniques et il suffit d'en vérifier la présence et la conformité sur le système réalisé.

Cette méthode a quatre inconvénients majeurs :

- En général, l'objectif de sécurité initial et les arguments techniques ayant présidé au choix et à la conception du moyen, ne figurent pas dans la règle et sont rapidement oubliés. On se contente d'appliquer la règle sans en connaître le bien fondé. Or l'évolution des techniques, des procédures d'utilisation, des conditions d'emploi peut rendre le moyen inutile ou même néfaste.
- Certains concepteurs ou utilisateurs se contentent d'appliquer la règle, même s'ils la savent inutile ou néfaste, pour se protéger sur le plan juridique. "En cas d'accident, je suis inattaquable puisque j'ai appliqué la règle prescrite !".
- Les rédacteurs des règles n'ont pas conscience de leur responsabilité en définissant, en lieu et place du concepteur, en dehors du contexte réel de création et d'utilisation du matériel, les moyens d'assurer la sécurité.
- Enfin, et c'est le défaut le plus grave, cette méthode sclérose totalement l'innovation en interdisant toute solution originale autorisée par l'évolution de la technique et des conditions d'emploi.

Donnons un exemple caricatural de ce type de défaut réglementaire.

Au cours des années 60 on imposait la règle suivante pour la conception des câbles liant, sur les planeurs, le manche aux gouvernes. "Si le cheminement du câble à l'intérieur de la structure impose des coudes de plus de 15°, il faut assurer cette déviation en installant une poulie folle". L'objectif, non précisé, était d'éviter des coincements de câbles par frottement ce qui aurait rendu l'appareil impilotable. Or un constructeur proposait de placer un guide enduit de téflon en lieu et place de la poulie. Il est évident que le règlement, écrit bien avant la guerre, ne pouvait envisager l'utilisation d'un matériau tel que le téflon. Le constructeur eut de grosses difficultés pour faire admettre que sa solution répondait à l'objectif, caché, de sécurité. La réponse de l'administration était "on ne peut certifier un planeur sans les poulies imposées par le règlement". Or un guide en téflon assure beaucoup mieux le glissement du câble, sans parties mobiles sujettes, elles aussi, à des défaillances. Bien entendu, la démonstration de sécurité nécessita de nombreux essais de validation de la solution (vieillissement et usure en particulier).

La seule méthode efficace pour éviter les défauts que nous venons de citer consiste à établir des règles imposant des objectifs de sécurité et non les moyens de les atteindre. Ce règlement doit être accompagné d'une liste de "moyens acceptables de démonstration de conformité". Ces moyens de démonstration sont, par exemple, des méthodes d'essai permettant de vérifier que l'objectif est atteint. La grosse difficulté réside dans la quantification des objectifs. On s'en tire généralement en imposant des performances au moins égales à celles des systèmes actuellement en service. Parmi les moyens de démonstration, on peut ajouter une ou des dispositions technologiques ayant fait leurs preuves, en en restreignant l'utilisation à la condition que les modalités d'emploi soient inchangées.

Cette méthode dite de réglementation par objectif a le gros avantage de laisser la porte ouverte à toutes les innovations. C'est au concepteur de montrer que sa solution conduit au même niveau de sécurité, ce qui reporte la responsabilité du choix des solutions sur le concepteur et non sur les services officiels qui n'en ont pas les moyens. C'est l'une des raisons pour lesquelles elle est souvent rejetée par les concepteurs qui trouvent plus confortable de ne pas assumer cette responsabilité et de la laisser à un service où elle se dissout dans l'anonymat.

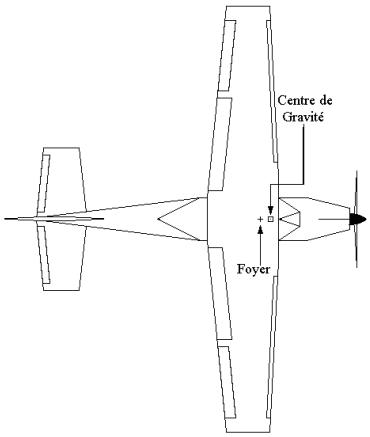
A titre d'exemple, citons le problème de sécurité lié à la résistance des pare-brise d'avion face aux impacts d'oiseaux. La méthode par moyens consiste à imposer un matériau et des méthodes de dimensionnement et de fabrication ayant fait leurs preuves sur des avions connus. La méthode par objectif impose seulement une méthode de démonstration de résistance à l'impact dans des conditions normalisées, vitesse d'impact, masse et taille des volatiles, ces conditions étant reconnues comme représentatives du risque maximal encouru raisonnablement probable.

Donnons quelques exemples supplémentaires.

- La réglementation impose aux responsables de chantiers sur la voie publique de signaler les travaux par des panneaux comprenant, entre autres, un panneau de limitation de vitesse à 50 km/h. Pour éviter de se voir imputer la responsabilité d'un accident au voisinage d'un chantier, les entrepreneurs de travaux publics posent alors un panneau de limitation de vitesse à coté de chaque tas de cailloux ce qui amène les automobilistes à les considérer comme superflus et rend la signalisation inefficace dans les cas, rares, où elle serait utile.
- L'accident ferroviaire d'Argenton sur Creuse a une origine réglementaire analogue. La présence de travaux importants sur la voie a conduit à la mise en place d'une profusion de signalisations d'alarme parfaitement réglementaires. L'abondance de ces signaux a provoqué une surcharge de travail temporaire sur le mécanicien qui n'a pas effectué le ralentissement nécessaire en temps utile et entraîné un déraillement fatal.
- Les organismes de certification des avions des États Unis avaient interdit l'emploi de systèmes hydrauliques pour actionner les gouvernes au moment de la mise en service des avions à réaction civils, estimant que ces systèmes n'étaient pas suffisamment fiables. Les concepteurs du Boeing 707 furent donc obligés de mettre en place un système purement mécanique très complexe de commandes de vol. Or des systèmes hydrauliques, qui avaient fait leurs preuves sur les avions militaires, auraient permis de résoudre simplement le problème des efforts aérodynamiques élevés dus aux grandes vitesses d'écoulement sur les gouvernes. Il fallut attendre sept accidents fatals en service avant que Boeing ne parvienne à maîtriser la complexité de son installation. Là encore l'administration avait imposé un moyen et non un objectif de sécurité.

  Fort heureusement cette interdiction ne fut pas maintenue ce qui permit d'installer des commandes hydrauliques sur des avions comme le DC8 et la Caravelle où la preuve de leur fiabilité fut établie.

- Citons un exemple plus complexe.

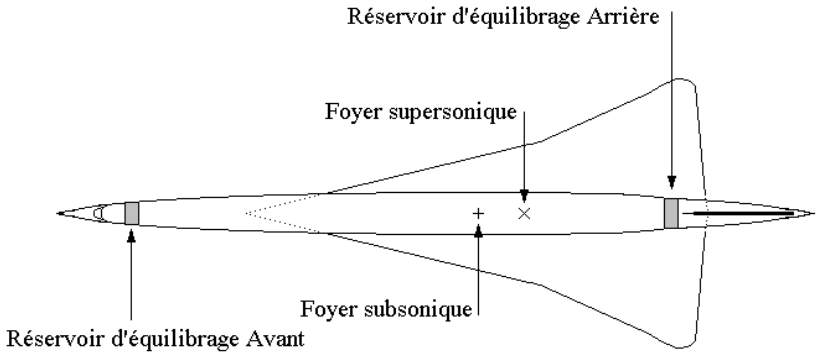


Un avion n'est stable que si son centre de gravité se situe en avant d'un point appelé foyer qui dépend principalement de la géométrie de l'aile.

Sur un avion classique à aile droite ce point se situe environ à 25% de la corde de l'aile en arrière du bord d'attaque. Pendant très longtemps le règlement stipula, avec juste raison, que l'on devait démontrer que l'avion était stable pour la position du centre de gravité la plus arrière que l'on peut rencontrer en vol. Il faut savoir en effet que le centre de gravité de l'avion se déplace au cours du vol et d'un vol à l'autre. Sa position dépend en effet de la répartition de la charge marchande (passagers et fret) le long du fuselage et de la consommation du combustible dans les différents réservoirs.

Or cette règle fut mise en défaut lors de la conception de Concorde.

Le foyer, fixe sur les avions subsoniques, n'a pas la même position sur les avions supersoniques selon que la vitesse est inférieure ou supérieure à la vitesse du son (lorsque l'avion vole à la vitesse du son, limite entre les deux régimes, il vole à un nombre de Mach égal à 1). Ce phénomène est dû au fait que l'écoulement de l'air autour de l'aile est très différent en régime subsonique (Mach inférieur à 1) et en régime supersonique (Mach supérieur à 1). Le foyer passe d'une position située, en régime subsonique, à environ 50% de la corde centrale de l'aile delta à une position située à environ 60% de cette même corde



en régime supersonique. Un avion centré de façon à être stable en subsonique (centre de gravité situé en avant du point à 50%) se trouve alors être trop stable en supersonique. Un tel centrage en avant du foyer subsonique conduit en supersonique à des positions de gouvernes en dehors du profil de l'aile générant une traînée aérodynamique prohibitive et une consommation de combustible interdisant la traversée de l'Atlantique. Il est donc nécessaire de reculer le centre de gravité de l'avion en régime de vol de croisière à Mach 2. Ceci est obtenu en déplaçant du combustible entre un réservoir situé à l'avant du fuselage et un réservoir situé à l'arrière. Dès lors l'avion, stable et correctement équilibré en supersonique, se trouve à un centrage qui le rendrait instable en subsonique. Aussi en fin de croisière, le combustible est-il transféré de nouveau de l'arrière à l'avant de façon à se retrouver en situation stable pour les manœuvres de descente et d'atterrissage.

Mais il est évident que la règle

"L'avion doit être stable avec la position du centre de gravité la plus arrière rencontrée en vol"

ne peut plus être satisfaite !

Ainsi l'évolution des techniques avait rendu caduque une règle qui s'était révélée judicieuse pendant les cinquante premières années de l'industrie aéronautique.

Il fallut des prodiges de rhétoriques pour convaincre l'administration américaine, par ailleurs peu disposée à accepter Concorde, de modifier le règlement pour tenir compte de ces nouvelles conditions d'emploi. La solution consista à démontrer qu'en cas de retour intempestif en régime subsonique à partir du vol de croisière (trois moteurs éteints fonctionnant en moulinet et un moteur bloqué, cas hautement improbable), il restait suffisamment d'énergie disponible à bord pour, au cours de la décélération

inévitable, ramener le centre de gravité, par transfert de combustible, en position acceptable en subsonique.

- Que dire des règlements administratifs, mal interprétés, imposant le verrouillage de locaux pour des raisons de secret militaire et interdisant de fait l'accès à des commandes de sécurité ou gênant l'évacuation en cas de catastrophe.

- Certains règlements fixent des limites aux doses d'exposition de la population et des travailleurs à des produits ou des radiations dangereuses. Ces règles sont nécessaires. Mais il faut prendre garde à ne pas céder à la tentation d'augmenter les exigences, sans de bonnes justifications, sous le prétexte d'améliorer la sécurité et sous la pression de l'opinion publique. Ainsi, après la catastrophe de Tchernobyl, certains pays ont exigé une radioactivité nulle pour tous les produits alimentaires! Or chacun sait qu'il y a partout une radioactivité naturelle non nulle (la dose apportée par Tchernobyl, en moyenne, en France, correspond à la dose reçue en quinze jours dans le Massif Central et en un mois et demi à Paris !)

Dans les conclusions du RAPPORT SUR LES CONSÉQUENCES DES INSTALLATIONS DE STOCKAGE DE DÉCHETS NUCLÉAIRES SUR LA SANTÉ PUBLIQUE ET L'ENVIRONNEMENT, on peut lire

> *Ceci va nous obliger à diminuer l'exposition des travailleurs du nucléaire en améliorant les procédés industriels et à faire tendre rapidement vers zéro les rejets de radioéléments dans l'environnement, une exigence que pointe un récent accord international certes non encore ratifié mais qui trace la seule voie d'avenir envisageable.*
>
> (C'est nous qui avons souligné les mots qui nous semblent sujets à critique)
>
> Cette démarche, louable dans ces intentions, est néanmoins utopique et dangereuse, ce qui est pour le moins fâcheux pour une mesure qui se veut augmenter la sécurité de l'humanité et de l'ensemble de la faune et de la flore mondiales.
>
> La sécurité dans le domaine de la production d'énergie nucléaire est un sujet délicat à aborder car il fait surgir des peurs incontrôlées reposant sur les vieux thèmes de l'apprenti sorcier ou de Frankenstein. Aussi allons-nous abandonner ce sujet controversé pour montrer par l'absurde, dans des domaines familiers, que la recherche du risque nul est utopique, inutile et même néfaste.

Chacun admet qu'un séjour prolongé sous l'eau se traduit par la mort. Il est dangereux de rester trop longtemps immergé. Le risque de périr noyé, c'est-à-dire la probabilité de se trouver dans ces conditions dangereuses d'immersion, est relativement faible dans la vie de tous les jours, du moins pour les citadins. Mais ce risque n'en est pas nul pour autant. Une collision sur le Pont Neuf peut projeter ma voiture dans la Seine et je peux rester coincé par la ceinture de sécurité qui refuse de se déverrouiller ! Le tunnel de la station Saint Michel peut se fissurer et la Seine peut envahir le réseau du métro. Je peux glisser en entrant dans ma baignoire, m'assommer et me noyer dans trente centimètres d'eau. Chacun va objecter que le risque de se trouver dans l'une de ces situations fâcheuses est complètement négligeable et c'est vrai. Il n'en reste pas moins que si je recherche un risque nul de noyade dans Paris, je ne peux me permettre de ne pas envisager ces situations (et bien d'autres que nous pouvons tout autant imaginer !). Pour se rapprocher du risque nul il serait donc judicieux que le Parlement vote une loi imposant le port obligatoire d'une brassière automatiquement gonflable au contact de l'eau. C'est techniquement possible, pourquoi s'en priver !

Autant mettre en place des moyens pour réduire un risque trop élevé jusqu'à une valeur raisonnable est judicieux, autant mettre en place des moyens coûteux pour réduire un risque déjà si faible qu'il est considéré comme négligeable, est totalement absurde.

Ainsi imposer la ceinture de sécurité à bord des voitures est-il judicieux car le risque de blessures graves ou mortelles est important en cas d'accident et la fréquence des accidents de la route est encore trop élevée. Par contre imposer le port de la brassière pour éviter la noyade en ville est pour le moins discutable.

Il est bien préférable de porter son effort sur des risques encore trop élevés dans la vie de tous les jours plutôt que de chercher à minimiser les risques déjà négligeables. Ainsi chercher à diminuer les risques dus à l'utilisation du gaz de ville, par explosions ou asphyxie, est beaucoup plus efficace que de chercher à limiter les risques de noyades. La réponse bien souvent est que l'une des mesures n'empêche pas l'autre et chacun de s'écrier "la sécurité n'a pas de prix". La réponse est bien connue "la sécurité n'a pas de prix, mais elle a un coût". Le coût d'une opération d'amélioration de la sécurité se mesure en Euros, mais en réalité ce sont des moyens en hommes et en matériels qui sont utilisés et les ressources ne sont pas illimitées. On ne peut

consacrer l'effort des soixante millions de français à la seule amélioration de sécurité. Il faut quand même en garder une bonne partie pour la production, le transport et la distribution.

Ainsi l'amélioration de la sécurité impose-t-elle un choix d'objectifs judicieux qui ne repose pas sur des sentiments et des raisonnements mal étayés, mais sur un vrai bilan coût efficacité afin de faire porter l'effort dans les domaines où la sécurité est encore insuffisante.

Il faut en outre se garder des risques imaginaires et éviter de prendre des mesures pour les couvrir.

Par ailleurs augmenter la sécurité dans un domaine peut se traduire par une diminution de sécurité dans un autre domaine. C'est ici que nous rencontrons l'aspect néfaste d'une mesure prise trop rapidement. Reprenons notre exemple absurde de brassière. Le gonflage intempestif de la brassière peut faire perdre le contrôle de la voiture et provoquer un accident mortel ! La gêne causée par le port de la brassière peut augmenter les embouteillages et bloquer le passage d'une ambulance, etc.

Une position raisonnable est la suivante.
Tant qu'un risque est bien identifié et jugé encore trop élevé, il est judicieux de mettre en place des moyens pour le réduire. Mais chercher à réduire encore un risque estimé négligeable n'est pas raisonnable car une telle opération se fait au détriment d'autres opérations plus utiles et peut même se révéler dangereuse dans d'autres domaines.

Encore faut-il s'entendre sur la notion de risque négligeable. Un risque doit être estimé négligeable s'il est considéré comme tel par un groupe d'experts indépendants par comparaison avec les risques naturels analogues que chacun encourt tous les jours (voir quelques réflexions sur le sujet dans le chapitre 15).

- Les règles doivent reposer sur des bases scientifiques sérieuses sous peine d'imposer des contraintes abusives et inutiles avec une double conséquence,

  - rendre le système économiquement non viable.

    Ainsi imposer de quadrupler tous les systèmes critiques sur les avions de transport réduirait la charge marchande d'un AIRBUS à quelques dizaines de places. Imposer une radioactivité nulle interdirait la consommation de tous les aliments.

  - imposer des solutions faisant courir d'autres risques.

    Ainsi, dans une unité de production chimique, réduire la quantité d'effluents gazeux polluant l'environnement, peut être obtenu en balayant l'installation avec un gaz inerte, azote ou gaz carbonique. Mais la présence de ces gaz peut conduire à des accidents graves et même mortels pour les travailleurs. On ne peut courir ce risque que si l'abaissement de la pollution est réellement nécessaire.

- Citons enfin la confusion fâcheuse qui règne dans les esprits des représentants de la puissance publique, des concepteurs et des utilisateurs en ce qui concerne les différences de statut entre les règles de sécurité imposées par la loi, les normes et l'homologation des matériels.

  Dans le domaine aéronautique un représentant de l'état a le devoir de vérifier l'application correcte des règles de sécurité imposées par le règlement de certification des avions. Ces règles relevant du domaine de la loi, il n'est pas question pour lui d'accorder des dérogations. S'il constate que la loi est défectueuse, il est de son devoir de le signaler et de demander une modification, mais cette dernière démarche relève du législateur et non du technicien seul.

  Dans certains cas, le règlement impose l'application de normes nationales ou internationales. L'application de ses normes devient alors obligatoire au même titre que les autres règles, mais seules ces normes sont obligatoires et le technicien responsable de la certification ne peut, de son chef, imposer l'application d'autres normes.

  Quelquefois, une démarche technique amène à exécuter des essais préliminaires sur des matériels, permettant d'en vérifier quelques performances. Si ces essais sont réussis, le matériel est dit homologué. Si le concepteur utilise ces matériels il est évident qu'il est inutile de répéter les essais d'homologation au

cours des essais de certification. L'utilisation de matériels homologués facilite donc la tâche de certification mais elle n'est ni imposable ni suffisante. Il faut en effet vérifier que les performances relevées dans les essais d'homologation sont conformes aux besoins de sécurité et que les conditions d'emploi des matériels homologués respectent également les règles de sécurité.

Enfin, il arrive que le même technicien responsable de la certification d'un avion civil, ait également la responsabilité de vérifier la conformité au cahier des charges des performances d'un avion de transport militaire commandé par l'État. Le cahier des charges imposera des règles de sécurité analogues à celles imposées aux avions civils, mais ces règles n'ont pas le même caractère. Les règles de certification des avions civils ont, rappelons le encore une fois, un caractère légal. Par contre, le cahier des charges d'un avion militaire n'est imposable au concepteur qu'à la suite d'un contrat passé par l'État client. Rien n'empêche le technicien, représentant de l'État client, d'imposer des règles plus sévères ou moins sévères que les règles de certification. En effet, les soucis de sécurité pour les avions militaires ne sont pas les mêmes que les soucis de sécurité pour les avions civils. Le technicien peut imposer, par contrat, l'application de normes autres que celles imposées par le règlement de certification et exiger l'utilisation de tel matériel homologué. Le technicien peut enfin accorder des dérogations aux exigences du cahier des charges. Il agit en effet dans le domaine contractuel en tant que représentant de l'État client et non dans le domaine légal en tant que représentant de l'État garant de la sécurité.

En définitive cette confusion des rôles de l'État client et de l'État garant de la sécurité conduit ainsi bien souvent à des Défauts Réglementaires.

CHAPITRE 11

GUIDE D'ANALYSE D'UN INCIDENT

GAFE (Grille d'Analyse des Facteurs d'Erreurs)
RADOS (Répertoire d'analyse des Défauts Opérationnels du Système)

GARE (Grille des facteurs Amplificateurs de Risque d'Erreur)
GASP (Grille d'Analyse des événements de Sensibilité aux Perturbations)
GAME (Grille d'Analyse des événements de Manœuvrabilité)

Ce chapitre reprend un grand nombre de notions développées dans les chapitres précédents de façon à pouvoir être lu de façon autonome et utilisé comme guide indépendant.

Les incidents décrits dans les fiches de RETOUR D'EXPERIENCE doivent être présentés sous forme de chaînes d'événements de trois types

- les événements d'Opérabilité mettant en cause les caractéristiques de l'opérateur humain,
- les événements de Sensibilité aux perturbations externes et internes,
- les événements de Manœuvrabilité caractérisant les manœuvres imposées par l'objectif de la tâche ou les manœuvres de corrections d'écarts.

La description des événements eux-mêmes, doit être précédée d'une description des conditions générales dans lesquelles se sont déroulés ces événements (conditions physiques telles que température, éclairage, visibilité, etc., conditions physiologiques, psychologiques et sociologiques des opérateurs.).

La connaissance de ces conditions est utile à deux titres.

- D'une part elles peuvent influer sur l'apparition des erreurs. Ainsi des températures extrêmes, une ambiance sonore intense, la fatigue, les soucis personnels, etc. réduisent les capacités des opérateurs et favorisent les erreurs, sans en être pour autant la cause directe. Elles agissent en tant qu'amplificateurs de gravité de la situation. Leur connaissance permet donc d'expliquer l'apparition d'erreurs aux cours d'événements d'opérabilité.
- Leur connaissance permet, d'autre part, d'estimer la probabilité de retrouver des conditions analogues en service et donc permet de juger l'utilité de trouver un remède pour limiter la probabilité d'apparition d'incidents du même type. Si ces conditions se révèlent exceptionnelles, on peut estimer qu'il n'est pas nécessaire de pousser l'analyse de l'incident jusqu'à la recherche de remèdes.

La GARE dresse la liste des principales conditions générales dans lesquelles se sont déroulés les événements, conditions agissant comme Amplificateurs du Risque d'Erreurs.

La GAFE est destinée à permettre d'identifier le Facteur d'Erreur caractérisant chaque événement d'Opérabilité.

Le facteur d'erreur ne caractérise pas à la nature de l'erreur elle-même commise par l'opérateur, mais plutôt les conditions particulières d'exécution de la tâche ayant favorisé l'apparition de l'erreur. Mis dans les mêmes conditions, divers opérateurs commettront des erreurs différentes, par exemple non-observation d'une déviation d'un paramètre important, mauvaise décision d'action, action intempestive ou non appropriée, oubli de transmission d'une information, transmission d'une mauvaise information, erreur de destinataire, etc.

Le RADOS est destiné à identifier le ou les Défauts du Système ayant contribué à l'apparition de chaque événement d'Opérabilité, quelquefois à l'apparition des événements des deux autres types et enfin à l'origine des conditions générales favorisant l'erreur.

La GASP est destinée à identifier le type de perturbation d'un événement de Sensibilité aux Perturbations.

La GAME est destinée à identifier le type de manœuvre exécutée au cours d'un événement de Manœuvrabilité.

Ces Grilles et le Répertoire ne peuvent être utilisés sans quelques explications complémentaires qu'il est impossible d'y faire figurer pour des raisons d'encombrement évidentes. Il est donc nécessaire de les compléter par un Guide, objet du présent exposé. Grilles et Répertoire sont donnés plus loin.

Ce Guide ne peut être utile qu'au spécialiste de l'analyse des fiches de RETOUR D'EXPERIENCE. Son contenu n'a rien de confidentiel, mais il est nécessaire de bien connaître les caractéristiques, bonnes et mauvaises, de l'opérateur humain pour être en mesure de l'utiliser avec profit. Il serait illusoire d'envisager de le confier aux rédacteurs des fiches en espérant les voir effectuer des analyses correctes et utilisables. Il constitue tout au plus un pense-bête permettant au spécialiste de conforter son analyse préalable en consultant les exemples d'erreurs typiques, ou les exemples de défauts du système illustrant chaque case de la Grille ou du Répertoire. Il devra être complété progressivement, par ce même spécialiste, à la lumière du retour d'expérience lui-même.

Une partie des considérations qui vont suivre ont été présentées dans les chapitres 9 et 10. Nous les reprenons afin d'obtenir un exposé complet qui peut être utilisé sans avoir à se référer à ces chapitres.

La Grille GAFE est constituée de quatre colonnes correspondant aux quatre types d'opérations rencontrées dans l'exécution de la tâche et de quatre lignes correspondant aux différents Facteurs d'Erreurs. La dernière ligne est divisée en cinq rubriques correspondant aux cinq types d'erreurs de représentation.

Le Répertoire RADOS est constitué des mêmes quatre colonnes et de cinq groupes de lignes correspondant aux différents types de Défauts des systèmes. A chaque Facteur d'Erreur identifiée par la GAFE, on peut faire correspondre un défaut système du Répertoire. On prendra garde au fait qu'il n'y a pas de correspondance automatique entre les Facteurs d'Erreurs repérées par la GAFE et les types de Défauts du RADOS (bien qu'il y ait généralement une forte corrélation, tel type de Défaut favorisant le plus souvent tel Facteur d'Erreur).

Les grilles GASP et GAME dépendent du type de Machine dont on étudie les incidents. Il est évident qu'un avion de transport est sensible à la turbulence de l'atmosphère, ce qui n'est pas le cas pour une motrice de TGV. Les perturbations internes, c'est-à-dire les pannes, sont spécifiques. Enfin, les manœuvres imposées par la mission ou les manœuvres de correction dépendent du type de machine étudiée. L'annulation du dérapage au moment du toucher des roues au cours d'un atterrissage par vent de travers (manœuvre dite de décrabe) est spécifique à l'avion de transport et n'a pas d'équivalent sur le TGV ou une centrale nucléaire. Aussi ne donnerons-nous, en fin d'annexe, les grilles GASP et GAME utilisées dans l'aéronautique qu'à titre d'exemple.

La grille GARE dépend elle aussi du type de Machine étudiée. Nous donnons toutefois, en fin de ce chapitre, une liste assez complète, bien que sans doute non exhaustive, des facteurs d'Amplification de Risque d'Erreurs les plus courants. Chaque utilisateur pourra éliminer les facteurs non adaptés à son cas particulier.

LES OPÉRATIONS D'EXÉCUTION DE LA TÂCHE.

L'étude des opérations exécutées par un opérateur, ou une équipe d'opérateurs, pour accomplir une tâche donnée, montre que ces diverses opérations sont de quatre types. Ainsi toute tâche peut être décrite par une succession d'opérations des types suivants, correspondant au mode de fonctionnement séquentiel dit "en canal unique" de l'opérateur.

- Saisie de l'information,
- Traitement de l'information aboutissant à une décision,
- Transmission de l'information,
- Action

(L'ordre de succession des opérations n'est pas systématiquement l'ordre indiqué ici, la décision pouvant par exemple être de saisir une autre information).

Saisie et traitement de l'information (sigle **s**)

L'opérateur capte une information par l'un de ses sens. Dans un processus industriel, la capture d'information se fait très généralement par les yeux (lecture d'un instrument, observation de l'environnement,...), souvent par l'ouïe (capture d'un message oral, reconnaissance d'un signal sonore, voire d'un bruit,...) ou par le toucher (reconnaissance de la forme, de la position d'une commande, évaluation de l'effort sur une commande,...), plus rarement par l'odorat (reconnaissance d'une odeur anormale,...) ou par le goût (eau plus ou moins salée,...).

La saisie de l'information nécessite:

⇨ la mise en service volontaire du capteur humain (opération cognitive)

⇨ la référence, plus ou moins consciente, à trois types de modèles stockés de façon plus ou moins parfaite dans la mémoire de l'opérateur (voir chapitres 3 et 4)

- → le modèle de localisation des sources d'information (pour savoir où capter l'information recherchée),
- → le modèle d'identification des sources d'information (pour pouvoir vérifier, si nécessaire, que la source d'information est bien celle souhaitée),
- → les modèles de transposition de l'information (ces modèles permettent de transformer une information brute, position d'une aiguille, couleur d'un voyant, forme d'un sigle ou d'une icône, en une information utilisable par le cerveau pour une décision ultérieure).

Il peut être utile de préciser si la source d'information est le système lui-même (transmission d'information Machine ⇨ Homme) ou un autre opérateur (transmission Homme ⇨ Homme). Si la source d'information est la machine, l'opération de saisie est déclenchée par une décision de l'opérateur (la décision pouvant être "forcée" par la machine dans le cas d'une alarme). Si la source d'information est un autre opérateur communiquant verbalement, l'opération de saisie est "forcée" par l'émetteur du message et l'information est en général fugitive. Les erreurs sont analogues dans les deux cas mais les défauts système à l'origine peuvent être très différents. Si nécessaire, le sigle **s** pour saisie sera complété du sigle **mh** (transmission d'information Machine ⇨ Homme) ou du sigle **hh** (transmission Homme ⇨ Homme).

Décision (sigle **d**)

Après avoir saisi une ou plusieurs informations, l'opérateur en fait une synthèse pour prendre une décision sur la suite à donner quant à l'exécution de sa tâche. La décision peut être de plusieurs sortes:

⇨ attendre, c'est-à-dire reporter à plus tard, avec un délai estimé, la capture d'autres informations (balayage des diverses informations disponibles ou capture d'un paramètre précis dont on prévoit la variation à terme),

⇨ saisir une autre information précise pour compléter la synthèse,

⇨ déterminer la commande sur laquelle on va agir, avec évaluation du sens et de l'amplitude de l'action sur la commande,

⇨ transmettre une information avec détermination de la nature du message, du mode de transmission et du destinataire.

La prise de décision nécessite la connaissance des Modèles de Fonctionnement du système à contrôler, c'est-à-dire les relations entre commandes, état de l'environnement et paramètres d'état du système. Elle nécessite également la connaissance des Modèles de Risque. Certaines décisions peuvent être prises à l'aide de procédures

qui facilitent l'interprétation des informations et le choix d'actions qui en résulte, sans passer par les modèles de fonctionnement du système.

Transmission de l'information (sigle **t**)

Les transmissions d'information sont multiples. Elles dépendent de la nature du message à transmettre, du moyen de transmission, du destinataire.

Les **messages** peuvent être

- ⇨ des messages oraux exprimés en langage naturel,
- ⇨ des messages exprimés en langage normalisé (message dont la forme et/ou le contenu ont été précisés par une règle générale de transmission),
- ⇨ des messages exprimés en langage codé (code alphabétique ALPHA pour A, ..., ZOULOU pour Z),
- ⇨ des messages réduits à la valeur d'un paramètre, valeur numérique, valeur binaire ou discrète, etc.

Les **moyens de transmission** sont également variés,

- ⇨ transmission orale, par sifflet, etc.
- ⇨ transmission à l'aide d'un clavier (clavier type ordinateur, pavés spécialisés, touche unique spécialisée, bouton poussoir de commande de la sirène d'alarme générale, etc.)
- ⇨ transmission par signaux optiques, par gestes, par pavillons, etc..
- ⇨ transmission par bâton pilote, etc.
- ⇨ transmission écrite manuelle, etc.

Le **destinataire** peut être

- ⇨ un autre membre de l'équipe (en vue directe ou non),
- ⇨ un opérateur ou un groupe d'opérateurs extérieurs,
- ⇨ l'opérateur lui-même pour une mémorisation de l'information à usage ultérieur.
- ⇨ un système de stockage de l'information
  - → introduction d'une valeur de consigne pour un automatisme
  - → entrée d'une donnée dans un historique
  - → entrée d'une donnée dans un cahier de signalement
  - → entrée dans une fiche de signalement d'avarie
  - → compte rendu d'événement (fiche RETOUR D'EXPERIENCE), etc.

La **transmission d'information** nécessite pour l'opérateur de disposer de modèles stockés de façon plus ou moins parfaite dans sa mémoire, à savoir des modèles (voir chapitres 3 et 4)

- ⇨ de localisation des moyens de transmission,
- ⇨ d'identification des moyens de transmission
  (pour pouvoir vérifier, si nécessaire, que le moyen de transmission est bien celui souhaité),
- ⇨ de mode d'action des moyens de transmission,
- ⇨ d'identification des organismes destinataires.

Il peut être utile de préciser si le destinataire de l'information transmise est le système lui-même (transmission d'information Homme ⇨ Machine) ou un homme (transmission Homme ⇨ Homme). Les erreurs sont analogues dans les deux cas mais les défauts système à l'origine peuvent être très différents.

Si nécessaire le sigle **t** pour transmission sera complété

du sigle **hm** (transmission d'information Homme ⇨ Machine)

ou du sigle **hh** (transmission Homme ⇨ Homme).

Action (sigle **a**)

L'opérateur actionne une commande, en général à l'aide de la main, d'un doigt, quelque fois avec le pied. Pour les opérations de maintenance les commandes peuvent être les divers outils, les commandes des outillages et les commandes des systèmes de contrôle et de mesure.

Toute action nécessite

- ⇨ la mise en service volontaire de l'actionneur humain (main, doigt ou pied), (opération cognitive),
- ⇨ la référence, plus ou moins consciente, à quatre types de modèles, stockés de façon plus ou moins parfaite dans la mémoire de l'opérateur, à savoir des modèles (voir chapitres 3 et 4)
  - → de localisation des commandes (pour savoir où se situe la commande désirée),
  - → d'identification des commandes (pour pouvoir vérifier que la commande saisie est bien celle souhaitée); ce modèle peut se réduire à la reconnaissance par la forme, la taille, la couleur.
  - → de mode d'action des commandes (pour savoir dans quel sens agir pour obtenir l'effet désiré, tirer, pousser, lever, tourner à gauche, etc.)
  - → de localisation du retour d'information sur l'état de l'organe commandé (l'état de l'organe commandé n'est pas toujours fourni par la position de l'actionneur lui-même; ainsi dans le cas d'une commande de vanne par bouton poussoir agissant sur un moteur d'ouverture ou de fermeture, il est nécessaire d'avoir une information sur la position de la vanne *elle-même*).

Certaines opérations de transmission d'information (par manipulation de claviers et de touches) s'apparentent à des actions sur des commandes. On prendra garde à ne pas les confondre. Une action a pour objet une modification de l'état du système, ce qui n'est pas le cas pour une transmission d'information (la distinction est subtile lorsque la transmission d'information est l'envoi d'une valeur de consigne à un automatisme).

Il faut enfin noter qu'une tâche peut être décrite par une succession d'opérations des quatre types décrits; mais, nous l'avons déjà dit, cette succession n'est pas systématiquement dans l'ordre Saisie d'information, Décision, Transmission et Action.

LES FACTEURS D'ERREURS (Grille GAFE).

⇨ **Les Facteurs d'Erreur liés aux caractéristiques et limitations anatomiques et physiologiques des opérateurs**

→ **Charge de travail** (sigle **C**),
La charge de travail est trop élevée, conduisant à un échec de l'opération par saturation des possibilités de l'opérateur.

→ **Lapsus** (sigle **L**) ou **maladresses**.
Les lapsus peuvent être gestuels (on accroche une commande avec la manche, on tape sur la touche d'à côté, on écrit une lettre à la place d'une autre ou on inverse les lettres d'une syllabe), verbaux (on prononce un mot à la place d'un autre), visuels (on "voit" un signal qui n'a pas été émis), auditifs (on entend une alarme qui n'a pas retenti).

⇨ **Les Facteurs d'Erreurs liés aux caractéristiques psychologiques des opérateurs**

→ **Absence de stimuli** (sigle **A**),
Le manque de stimuli en provenance du système conduit à une perte de vigilance de l'opérateur.

→ **Erreur de Représentation ou Conscience Erronée de la Situation.**

Ces facteurs d'erreur peuvent être divisés en cinq groupes,

→ Une Image Présente, Externe ou Interne, est erronée (Sigle **SPE** ou **SPI**)
La mauvaise image provient en général d'une mauvaise saisie d'une information ou d'un message.
→ Une Image Future, Externe ou Interne, est erronée (Sigle **SFE** ou **SFI**)
La mauvaise image provient en général de l'utilisation d'un modèle de fonctionnement erroné.
→ Une Image Désirée, Externe ou Interne, est erronée (Sigle **SDE** ou **SDI**)
La mauvaise image provient en général de l'utilisation d'un mauvais modèle de tâche.
→ Utilisation d'une Image, Externe ou Interne, "a priori" (Sigle **SAE ou SAI**)
Refus de l'information qui permettrait de rétablir la vérité.
→ Utilisation d'un mauvais Modèle de Risque
Les images présentes, futures et désirées sont exactes mais l'opérateur sous estime le risque lié à la situation. Pour une mauvaise estimation du risque correspondant à la situation externe sigle **SRE**. Pour une mauvaise estimation du risque correspondant à la situation interne sigle **SRI**.

⇨ Enfin il faudrait ajouter une dernière ligne portant le sigle **X** pour couvrir les cas qui n'entreraient dans aucune des rubriques précédentes, dans la mesure où nul ne peut prétendre à l'exhaustivité. Bien entendu, une erreur ne peut être classée dans cette dernière ligne qu'avec des justifications appropriées et une révision de la grille doit être proposée pour couvrir les cas analogues.

GRILLE D'ANALYSE DES FACTEURS D'ERREURS

GAFE

		Opérations d'exécution de la tâche au cours de laquelle survient l'erreur			
FACTEUR D'ERREUR ⇩		Saisie et traitement de l'information s	Décision après traitement de l'information d	Transmission de l'information t	Action après décision a
		Homme ⇩ Homme (hh) / Machine ⇩ Homme (mh)		Homme ⇩ Homme (hh) / Homme ⇩ Machine (hm)	
CHARGE DE TRAVAIL C Charge trop élevée Saturation		Cs	Cd	Ct	Ca
ABSENCE DE STIMULI A Perte de vigilance		A			
LAPSUS L		Ls	Ld	Lt	La
CONSCIENCE ERRONÉE de la SITUATION S	Image en cause				
Image Présente Erronée	Externe	SPEs	SPEd	SPEt	SPEa
	Interne	SPIs	SPId	SPIt	SPIa
Image Future Erronée	Externe	SFE			
	Interne	SFI			
Image Désirée Erronée	Externe	SDE			
	Interne	SDI			
Image A Priori	Externe	SAE			
	Interne	SAI			
Modèle de Risque Erroné	Externe	SRE			
	Interne	SRI			

UTILISATION DE LA GRILLE GAFE.

Pour chaque événement d'Opérabilité, il faut se poser deux questions,

- dans quelle catégorie se classe l'opération de déroulement de la tâche au cours de laquelle s'est produit l'événement, autrement dit dans quelle colonne de la grille se situe l'événement décrit ?
- sous quelle rubrique se classe le Facteur d'Erreur d'Opérabilité étudié, autrement dit dans quelle ligne de la grille le plaçons-nous ?

Dans bien des cas il est impossible de choisir une case unique pour caractériser l'événement parce que l'on manque d'informations. Ainsi, seul l'opérateur peut préciser, par exemple, qu'il a saisi la mauvaise commande parce que sa charge de travail était trop élevée (Ca), parce qu'il utilisait un mauvais modèle de localisation des commandes (SPIa) ou par suite d'une simple maladresse (La). Dans le doute, il faut caractériser l'événement par les trois sigles possibles (Ca ou SPIa ou La). Enfin, la reconnaissance d'une maladresse simple n'est à envisager que si l'on peut éliminer les trois autres cas possibles (C, A, S).

Par ailleurs le choix de la colonne ne fait qu'identifier l'opération au cours de laquelle l'erreur s'est manifestée.

Dans bien des cas le fait qu'une erreur survienne à l'occasion de telle ou telle opération n'est qu'anecdotique. Mis dans les mêmes conditions un autre opérateur ou le même opérateur commettrait une erreur à l'occasion d'une opération d'un autre type.

Ceci est toujours le cas pour le Facteur d'Erreur Absence de Stimuli conduisant à la chute de la vigilance. Dans ce cas, il est inutile en conséquence de préciser la colonne et le sigle caractérisant le Facteur d'erreur se réduira à A sans plus de précision.

C'est souvent vrai pour le Facteur d'Erreur Charge de Travail élevée. Néanmoins il peut être utile de préciser la colonne pour pouvoir vérifier ultérieurement, lors de la comparaison de plusieurs incidents du même type, si l'erreur ne survient pas quasi systématiquement pour le même type d'opération, ce qui peut être un guide utile pour déterminer le type de Défaut Système en cause. Si par exemple on constate que l'erreur survient souvent au cours d'une saisie d'information, il faut vérifier si la procédure ne conduit pas à une surcharge de travail en exigeant de nombreux relevés de paramètres dans un temps trop court.

La précision de l'opération en cours est très utile dans le cas du Lapsus car le type d'opération en cause caractérise le type de lapsus, visuel, verbal, auditif ou gestuel. Par exemple un lapsus gestuel peut être l'indication d'une mauvaise disposition des commandes favorisant une maladresse.

Enfin dans les cas de la Conscience Erronée de la Situation, la précision de la colonne n'est utile que pour la première rubrique, Mauvaise Image Présente, pour préciser au cours de quelle opération, saisie d'information, transmission d'information, action, la fausse image a été forgée. Pour les quatre autres rubriques préciser la colonne ne fait que signaler au cours de quelle opération l'erreur est survenue, ce qui n'est qu'anecdotique et ne caractérise pas le Facteur d'Erreur.

Dans certains cas il est difficile, par manque d'information à la lecture du rapport d'incident, de préciser la colonne de la grille. On remplace alors les sigles s, d, a et t par le sigle *.

EXEMPLES ILLUSTRANT L'UTILISATION DE LA GRILLE GAFE.

⇨ COLONNE (s) Saisie et traitement de l'information

→ CHARGE de TRAVAIL TROP FORTE (Cs)

→ Au cours d'une opération de conduite, l'opérateur doit, dans un temps réduit, exécuter trop d'opérations pour accomplir la tâche requise (par exemple reconfiguration rapide après panne). Il n'observe pas une variation significative sur un paramètre important en dehors de son champ d'action immédiat.

→ Au cours d'une opération de maintenance corrective à effectuer dans un temps limité pour des raisons de délai de retour à la disponibilité opérationnelle, l'opérateur se trompe en relevant une valeur de contrôle à vérifier avant de poursuivre sa tâche.

→ LAPSUS (Ls)

→ Lecture erronée d'une étiquette, par exemple CR00012 au lieu de CR00021, bien que l'étiquette soit parfaitement éclairée et correctement écrite.

→ L'opérateur croit entendre un message d'alarme alors que ce n'est qu'un bruit sans signification.

→ L'opérateur croit entendre le message "OUI" en réponse à une interrogation alors que son interlocuteur a répondu "QUI"

Il est parfois difficile de faire la différence entre ce type d'erreur, très courante dans la vie de tous les jours, et l'erreur de modèle a priori (SA) pour laquelle l'opérateur "ne lit ou n'entend que ce qu'il s'attend à lire ou à entendre"

"Le robinet CR0012 doit être ici"; je vois l'étiquette CR0021 et je me dis "c'est bien ce que je pensais, voici le robinet CR0012".

"La situation est délicate! d'ici qu'une alarme retentisse il n'y a pas loin"; j'entends un bruit et me dis "c'est bien ce que je pensais, voilà l'alarme".

"Le collègue doit normalement me répondre OUI"; j'entends un bruit et je me dis" c'est bien ce que je pensais, il est d'accord".

→ CONSCIENCE ERRONEE DE LA SITUATION (SPs)

→ L'opérateur oublie de renouveler son image mentale de la situation et raisonne sur une image "vieillie" qui ne reflète plus la réalité, certains paramètres ayant changé. "Il n'y a aucun obstacle autour du véhicule, je l'ai vérifié (en réalité cette vérification date de quelques instants et la situation s'est modifiée); je peux donc effectuer ma manœuvre en toute sécurité !". (SPes)

→ Le courant a été coupé et l'opérateur l'a vérifié il y a plusieurs minutes. Il ne pense pas à le vérifier à nouveau avant une nouvelle intervention, alors que la tension a été rétablie, entre temps, par un autre opérateur. (SPIs)

→ L'opérateur confond, lors d'une opération d'échange d'essieu sur une voiture SNCF, le repérage par rapport au boggie et le repérage par rapport à la voiture (mauvais modèle de repérage). (SPEs)

→ L'opérateur se trompe d'instrument de contrôle; il lit la température à relever sur le troisième thermomètre et non sur le quatrième. (SPIs)

C'est le cas typique d'erreur de modèle de localisation de la source d'information dont les origines possibles sont multiples (voir les exemples RADOS),

- entraînement sur un pupitre simulé non conforme au pupitre opérationnel (l'opérateur est "intellectuellement" au fait de cette différence mais le réflexe acquis à entraînement l'emporte sur la connaissance), (Défaut Système Fss)
- disposition des instruments sur le panneau en contradiction avec la disposition spatiale des points de mesure sur le système réel ou sur le schéma de conduite (Défaut Système Hcs).

Ce type d'erreur peut être aggravé par une erreur du modèle d'identification des sources d'informations si la distinction entre une dizaine d'instruments de mêmes formes ne peut se faire que par lecture d'un étiquetage ésotérique; par exemple étiquettes K22A, K22B, K22C,..... pour des points de mesure repérés sur le schéma T421, T422, T423,....cet état de fait malheureux provenant du fait que les numérotations sur le pupitre et sur le schéma de conception, utilisé pour la conduite, ont été faites par des responsables n'ayant pas les mêmes préoccupations et surtout pas celle de la conduite (Défaut Système Hcs).

→ L'opérateur relève une valeur erronée d'un paramètre parce qu'il n'a pas noté la position d'un commutateur de changement d'échelle. Il interprète la position de l'aiguille avec une mauvaise échelle erreur de modèle de transposition). (SPIs)

→ Un bouton poussoir permet, à chaque appui, de modifier la valeur de l'échelle de mesure et/ou le type de paramètre mesuré. Le résultat de cette action est affiché en bonne et due place, mais l'opérateur ignorant la dernière action sur le poussoir (de sa part ou, plus grave, de la part d'un autre opérateur) oublie de consulter cette information sur l'indicateur auxiliaire et interprète à tort l'information transmise par l'indicateur principal (erreur du modèle de localisation ou erreur de modèle de transposition). (SPIs)

→ L'opérateur relève une valeur erronée d'un paramètre parce qu'il se trompe sur la valeur du zéro de l'échelle (c'est le seul instrument du panneau dont la graduation débute à 20 et non à zéro) (erreur de modèle de transposition). (SPIs)

→ Au cours d'une opération de maintenance**,** l'opérateur relève une valeur erronée à l'aide de son multimètre car il a oublié que l'échelle des ohms est croissante vers la gauche (erreur de modèle de transposition). (SPIs)

→ Au cours d'une opération de maintenance l'opérateur relève la tension en un mauvais point du circuit (erreur de modèle de localisation de la source d'information). (SPIs)

→ LAPSUS (Ld)

→ L'opérateur a bien analysé la situation mais il prend la décision contraire ou toute autre décision par "confusion mentale". L'opérateur a identifié que le bogie avant était défectueux et il démonte le bogie arrière tout en pensant qu'il fait attention à démonter "le bon".

Il est souvent difficile de distinguer ce type de lapsus du lapsus d'Action (La) ou du lapsus de saisie de l'information (Ls).

→ CONSCIENCE ERRONEE DE LA SITUATION (SPd)

→ Le pilote ayant lu le cap 80 (alors que le cap réel est 30) décide de virer à gauche pour rejoindre le cap 50. (SPEd)

→ Le pilote ayant vu basculer l'aiguille du radio compas pense avoir passé la verticale de la balise et décide la mise en descente alors que le basculement est le résultat d'un éclair d'orage. (SPEd)

→ **c**entrale de Three Mile Island. Une panne des turbines provoque l'absence de refroidissement du circuit secondaire et donc une surchauffe du circuit primaire imposant l'arrêt d'urgence automatique (chute des barres, ouverture d'une vanne de décharge pour limiter la surpression transitoire). Douze secondes après le début de chute des barres, les automatismes envoient, comme prévu, l'ordre de fermeture de la vanne de décharge. Celle-ci est signalée refermée, mais un incident mécanique la maintient ouverte. Le chef de quart se fait donc une image fausse de l'état du cœur (en train de se vider) et il prend la décision, fâcheuse, mais logique pour lui, de couper l'alimentation de secours en eau déclenchée par les automatismes qui ont détecté une baisse de niveau dans le cœur. (SPId)

⇨ COLONNE (t) Transmission de l'information

→ CHARGE de TRAVAIL TROP FORTE (Ct)

→ l'opérateur ayant à transmettre un message urgent pendant une période "chargée", ne transmet pas le message, en transmet un erroné, se trompe de destinataire ou de canal de transmission.

→ LAPSUS (Lt)

→ C'est le cas le plus classique du lapsus verbal. On pense qu'il faut commander une manœuvre "à gauche" et l'on prononce "à droite". On commande "à descendre" alors que l'on pense attentivement à bien commander "à monter". C'est également le cas du lapsus gestuel que l'on retrouve aussi en La; on appuie sur la mauvaise touche ce qui conduit à une erreur de destinataire (qui n'a pas fait de faux numéro au téléphone sans que la Poste soit en cause).

→ CONSCIENCE ERRONEE DE LA SITUATION (SPt)

→ L'opérateur se fait une fausse image de l'état du système de transmission. Il émet son message sur "public adress" et non sur la fréquence du contrôle de circulation aérienne. Il pense émettre alors que l'émetteur est en panne. Il émet sur une mauvaise fréquence, etc.

⇨ COLONNE (a) Action

→ CHARGE de TRAVAIL TROP FORTE (Ca)

→ Au cours d'une opération de conduite, l'opérateur doit, dans un temps réduit, exécuter trop d'opérations pour accomplir la tâche requise, reconfiguration après avarie par exemple. Il rate ou oublie d'effectuer une action sur une commande ou encore se trompe de commande.
→ Au cours d'une opération de maintenance corrective à effectuer en temps limité pour des raisons opérationnelles, l'opérateur se trompe de pièce à échanger et laisse la pièce défectueuse en place.

→ LAPSUS (La)

→ C'est le cas le plus classique du lapsus gestuel. On veut atteindre une commande un peu éloignée et l'on accroche au passage une autre commande. Sur mouvement inattendu de plate-forme, une commande ou une action "de travers" est enclenchée. C'est souvent ce genre d'erreur qui figure implicitement dans les rapports d'incidents derrière les vocables "maladresses" ou "action malencontreuse". Il est parfois bien difficile à l'analyse de faire la différence entre l'erreur gestuelle et l'erreur de modèle de localisation des commandes.

→ CONSCIENCE ERRONEE DE LA SITUATION (SPa)

→ L'opérateur agit sur le troisième levier au lieu du quatrième (erreur de modèle de localisation des commandes),
→ L'opérateur ferme une vanne en tournant le volant dans le sens classique alors qu'il est en présence d'une vanne particulière qui se ferme en sens inverse (erreur de modèle de sens d'action),
→ L'opérateur ferme CJ 00120 au lieu de CJ00012 par mauvaise identification de la commande (erreur de modèle d'identification des commandes),
→ L'opérateur vérifie le résultat de son action sur une vanne par l'intermédiaire d'un poussoir actionnant un moteur de fermeture et se trompe d'indicateur de retour de position.

Les deux dernières erreurs sont à rapprocher des erreurs de saisie d'information mais résultats et remèdes sont différents.

⇨ FACTEURS D'ERREUR INDEPENDANTS DU TYPE D'OPERATION

→ ABSENCE de STIMULI, Perte de Vigilance (A)
→ L'opérateur placé devant un panneau de contrôle dont les informations sont figées depuis plusieurs heures, ne note pas la dérive d'un paramètre important ou l'apparition d'une signalisation ou encore n'agit pas sur une commande au moment requis parce que sa vigilance est amoindrie par une situation non évolutive ne lui fournissant aucune information intéressante.
→ Surveillance du scope de contrôle pour la détection des fissures d'essieu, avec une détection très rare d'anomalie.
→ Surveillance du scope radar pour assurer l'anticollision avec les autres navires, avec une détection très rare d'objectifs.
→ Au cours d'une opération de maintenance un opérateur laisse déborder un réservoir car l'opération de remplissage se déroule depuis de longues minutes, sa seule tâche étant d'attendre la fin de cette opération.
→ La situation est stable et l'opérateur en conclut qu'elle va le rester et qu'il n'est pas nécessaire de surveiller le processus. Il peut aussi faire un diagnostic réflexe reposant sur une erreur de reconnaissance de la situation.
→ L'opérateur, ayant à transmettre un message de routine au cours d'une attente "sans rien à signaler", ne transmet pas le message, transmet un message erroné ou se trompe de destinataire. Il peut également se tromper de canal de transmission par erreur de touche.

→ CONSCIENCE ERRONEE DE LA SITUATION. Image future erronée. (SF)
→ L'opérateur utilise un modèle faux, dû par exemple à une formation inadaptée ou à un modèle simpliste. Il utilise ainsi un modèle général de fonctionnement du système, valable dans 95% des cas, alors que la

situation du système exigerait un modèle plus élaboré ou un modèle différent (voir Défaut Système Fsd).

→ Le pilote pense que sa trajectoire montante lui permettra de passer l'obstacle mais il surestime les performances de son avion.

→ Le conducteur freine tardivement parce qu'il surestime les capacités du système de freinage (il pense que le système ABS réduit les distances de freinage).

→ Le conducteur pense que la distance de freinage à 100 km/h est seulement le double de la distance de freinage à 50 km/h.

→ CONSCIENCE ERRONEE DE LA SITUATION. Image désirée erronée. (SF)

→ Après décollage le pilote vire à gauche en suivant la procédure habituelle, mais exceptionnellement le contrôle a demandé un virage à droite. (SFE)

→ L'opérateur chargé du reprofilage des roues au tour en fosse ne change pas les données de référence en passant d'un modèle à un autre. (SFI)

→ Alors que le contrôle a imposé un changement de piste tardif pour une piste plus courte et avec vent défavorable, l'équipage ne change pas les vitesses caractéristiques de décollage (vitesse de décision d'abandon ou de poursuite du décollage, qui dépend de la longueur de la piste et des force et direction du vent)

→ L'opérateur démonte le troisième disjoncteur et non le quatrième parce qu'il est convaincu que c'est le troisième qui commande le système défaillant dont il a la réparation à charge. Il raisonne sur un modèle fonctionnel inadapté. (SFI)

→ L'opérateur utilise un système de transmission inadapté à la situation. Il se trompe de destinataire (il transmet à la hiérarchie au lieu du collègue) ou de nature de message (il croit nécessaire de transmettre telle information alors que le destinataire en attend une autre). Il se trompe de moyen de transmission (message oral au lieu de message écrit). Il estime qu'il suffit de transmettre sur un réseau de diffusion générale, sans préciser son code émetteur ni celui du destinataire, ni s'assurer de l' "Accusé de réception" ("A toi").

→ CONSCIENCE ERRONEE DE LA SITUATION. Image "a priori". (SA)

→ Au cours d'une opération de conduite ou de maintenance, l'opérateur lit une valeur erronée ou interprète faussement une indication par voyants parce qu'il est convaincu que la valeur relevée ou la signalisation "doit être normale " puisque la situation était jusqu'à présent normale et qu'il a, pense-t-il, effectué correctement les opérations nécessaires.

→ Au cours d'une opération de maintenance, l'opérateur remplace successivement plusieurs exemplaires d'un même système, les jugeant tous défectueux, alors que la panne vient d'ailleurs.

→ Au cours d'une opération de maintenance, l'opérateur met en place un système sortant de révision. Il le juge "bon" a priori et cherche la panne ailleurs si une anomalie est détectée.

→ L'opérateur mesure la tension sur un circuit normalement coupé et interprète ce qu'il lit sur le voltmètre comme une erreur de l'instrument et non comme la présence réelle d'une tension. (exemple de mauvaise utilisation du VAT Vérificateur d'Absence de Tension).

→ Au moment précis d'une action sur une commande une alarme survient. L'opérateur ne pousse pas le diagnostic plus loin et attribue la cause de l'anomalie à son action. (SAI).

→ L'opérateur sait qu'une panne est déjà survenue. Un fonctionnement anormal survient, accompagné ou non d'une alarme. L'opérateur attribue ce dysfonctionnement à la panne connue sans faire un diagnostic plus approfondi ("ça y est, ça recommence !). (SAI)

→ L'opérateur refuse d'admettre la réalité d'un feu moteur. Il invoque un mauvais fonctionnement des alarmes. En un mot il considère que "cela ne peut lui arriver, à lui qui n'a jamais eu de pépins".

→ Au cours d'une opération de maintenance dans un atelier de la RATP, un opérateur ayant terminé sa tâche sur fosse, transmet l'information "train bon", puis, constatant qu'il a oublié d'effectuer une opération, coupe à nouveau le courant, verrouille le disjoncteur avec le cadenas et retourne dans la fosse sans prévenir. Le conducteur chargé de sortir le train, sachant "a priori" le "train bon" croît que l'opérateur a oublié de remettre le courant et de retirer le cadenas; il rétablit la tension en "court-circuitant" la sécurité imposée par le cadenas.

→ L'opérateur peut également ne tenir compte que des informations confirmant le modèle a priori qu'il s'est forgé (j'ai coupé le disjoncteur et ai vérifié sa coupure; le voltmètre est donc faux et je n'en tiens pas compte; le cadenas est en place, mais je connais l'opérateur, il est étourdi et ce jour là très pressé de rentrer chez lui !).

→ Dans le même esprit, on remarquera que bien souvent, à la lecture d'un compte-rendu de réunion, on constate que les divers participants n'ont entendu que ce qu'ils désiraient entendre.

→ CONSCIENCE ERRONEE DE LA SITUATION. Modèle de risque erroné. (SR)

- → L'opérateur ne reconnaît pas la gravité de la situation parce qu'il ignore être dans un cas dangereux. Il ignore que telle vibration dans telle partie de la structure est dangereuse, alors qu'une vibration de même amplitude et de même fréquence est anodine, il en a fait l'expérience, en d'autres endroits.
- → L'opérateur de maintenance ne débranche pas la pompe à graisse, ignorant le danger de travailler à proximité.
- → Le pilote d'avion léger ne met pas en route la pompe de gavage au décollage, car il estime négligeable le phénomène de vapor lock (bulle de gaz dans le circuit de carburant, bloquant l'arrivée d'essence au moteur et provoquant son arrêt).
- → Le pilote se pose avec une vitesse excessive, sur une piste courte et mouillée, avec vent arrière sachant qu'il a déjà rencontré séparément de telles situations mais en oubliant que la conjonction de ces trois événements conduit à un risque sérieux.
- → Le pilote traverse un gros nuage d'orage en estimant que la turbulence et la foudre ne sont pas aussi dangereux qu'on veut bien le dire.
- → Un plaisancier s'aventure à traverser le Pas de Calais dans le brouillard en coupant la route des navires de commerce.
- → Un alpiniste amateur se lance dans une course en montagne sans aucun équipement.

On remarquera que l'accident de TCHERNOBYL est particulièrement instructif. On y rencontre les cinq types de Conscience Erronée de la Situation !

On notera par ailleurs qu'il ne faut pas s'imaginer que l'opérateur est conscient de ces comportements aberrants et en déduire une présomption de faute. Rappelons qu'il est hors de sujet du présent guide d'émettre des jugements ou des justifications de comportement. Un observateur extérieur peut s'étonner de voir des opérateurs sérieux et consciencieux se comporter ainsi mais il doit se convaincre que le raisonnement des opérateurs plongés dans cette situation d'erreur diabolique est parfaitement logique; ce raisonnement repose sur des hypothèses fausses difficiles à remettre en cause dans le feu de l'action.

LES TYPES DE DÉFAUTS SYSTEME (Répertoire RADOS)

Les types de Défauts sont regroupés en cinq classes.

⇨ la **mauvaise organisation** du travail de l'équipe, de l'unité, de la direction, de l'entreprise, etc. (sigle **O**).
Ces défauts se divisent eux-mêmes en quatre catégories

⇨ *les opérateurs ne savent pas ce qui est de leur responsabilité*, ce qu'ils doivent faire eux-mêmes, ce qu'ils ne doivent pas faire, ce qu'ils peuvent déléguer, quelles informations ils doivent transmettre. En conséquence, ils omettent une opération croyant qu'elle n'est pas de leur ressort ou exécutent une action normalement impartie à un autre opérateur. Ce type d'erreur est bien souvent à l'origine d'une erreur de représentation pour un autre opérateur.
(Réponse à la question *Qui doit faire ?*, sigle complémentaire **r** pour responsabilité)

⇨ *les définitions des objectifs, des contraintes, des marges disponibles comportent des erreurs, ce que nous regrouperons sous le terme de Tâches mal définies.* En particulier, les situations nominales recommandées sont trop près des limites, ce qui laisse des marges trop faibles pour couvrir les aléas (erreur d'Opérabilité, Perturbations, Manœuvres). Ou encore l'opérateur se définit un objectif de tâche qui ne lui a pas été prescrit ("faire l'heure", "atterrir a tout prix",etc).
(Réponse à la question *Que doit-on faire ?*, sigle complémentaire **e** pour exécution)

⇨ *les opérateurs ne disposent pas de moyens suffisants,* en personnel ou en matériel, pour exécuter leur tâche. Cela conduit en général à des surcharges de travail, quelque fois de courte durée, mais suffisantes pour conduire à l'erreur. Ce cas se rencontre souvent dans les postes de travail à charge moyenne faible ne justifiant pas un nombre d'opérateurs suffisant pour faire face aux pointes.
Tâche prévoyant des transmissions d'informations alors que les moyens de transmission ne sont pas disponibles (centre de contrôle fermé la nuit par exemple).

(Réponse à la question *Quels moyens pour faire ?*, sigle complémentaire **m** pour moyen)

⇨ *les opérateurs ne savent pas comment exécuter leur tâche* ou encore les procédures qu'on leur impose sont mal adaptées aux caractéristiques de l'opérateur humain et aux moyens dont ils disposent en homme et matériel.
(Réponse à la question *Comment faire ?*, sigle complémentaire **p** pour procédure)
Cette situation a des origines multiples,
- procédures matériellement défectueuses (erreurs de frappe, photocopie imparfaite, etc.),
- procédures imparfaites parce que mal rédigées, complexes, non expliquées,
- procédures trop générales laissant l'opérateur devant un choix difficile à faire,
- procédures imposant des charges de travail ponctuelles trop élevées ou imposant des tâches fastidieuses (longs temps d'attente entre opérations, attente d'un événement qui ne se produit que très rarement, surveillance sans événements notoires) néfastes à la vigilance (attention il ne s'agit pas de charger les opérateurs par des opérations artificielles ou inutiles !), etc.

Cela se traduit le plus souvent par des opérations manquées à l'origine d'erreurs de représentation pour l'opérateur lui-même ou pour un autre opérateur qui pense que la tâche de son collègue a été correctement exécutée.

Il est à noter qu'il est quelquefois difficile de distinguer les défauts de type **e** (Que doit-on faire ?) des défauts de type **p** (Comment doit-on faire ?). Est-ce la procédure qui traduit mal la tâche ou est-ce la tâche qui a été mal définie ? Il est toutefois important de faire la distinction car les remèdes sont différents.

⇨ la **mauvaise conception de la machine** (sigle **H**)

La conception de base repose sur des hypothèses ne prenant pas en compte toutes les situations envisageables et conduit dans certains cas, rares mais possibles, à des situations dangereuses.

La conception des interfaces ne tient pas compte des caractéristiques physiques, physiologiques ou psychologiques de l'opérateur moyen.

Les interfaces sont les pupitres d'instruments, les pupitres de commandes, les transparents isolant le poste de commande du monde extérieur, les moyens d'observation de l'environnement, les moyens de communication entre les opérateurs, les textes de consignes et de procédures.

Ces défauts peuvent être divisés en trois groupes,

→ mauvaise conception de base
(sigle complémentaire **b** pour base)
Structure ne résistant pas dans des conditions particulières, automatismes conduisant à des situations dangereuses, ..

→ mauvaise conception de l'interface sur le plan ergonomie mécanique
(sigle complémentaire **m** pour mécanique)
Éclairage, chauffage, ventilation, sièges, disposition, taille des afficheurs, disposition, taille, forme, débattements des commandes, disposition, forme, taille, couleur, caractères des étiquettes, ..

→ mauvaise conception de l'interface sur le plan ergonomie mentale
(sigle complémentaire **c** pour conception)
Échelles, zéros des afficheurs, sens d'action des commandes, synoptiques, schémas sur écran, ..

⇨ la **mauvaise conception de la formation** (sigle **F**)

Ces défauts peuvent être divisés en deux groupes,

→ mauvaise conception de la formation de base
(sigle complémentaire **b**)
- méconnaissances dans le domaine de la formation élémentaire, lecture, écriture, calcul mental, arithmétique, langage parlé ou écrit, etc.
- méconnaissances dans le domaine des techniques, mécanique, physique, électricité, électronique, informatique, aérodynamique, hydraulique, résistance des structures, usinage, soudure, langage technique, etc.
- méconnaissances de l'organisation générale de l'entreprise et de ses objectifs, des règles générales de transmission de l'information, des règles de sécurité, méconnaissances en matière de facteur humain, etc.

→ mauvaise conception de la formation spécifique au système
(sigle complémentaire **s**)
méconnaissances
- des modèles de fonctionnement du système conduisant à des erreurs de décisions,
- des modèles utilisés pour la captation d'information,
- des modèles utilisés pour l'action sur les commandes,
- de l'organisation en cours (répartition des tâches),
- des procédures,
- manque d'entraînement ou mauvaises méthodes d'entraînement,
- mauvaise mise à jour des connaissances (formation continue).

⇨ les **Défauts de conception ou de réalisation de la Documentation,**
les **Informations erronées, non transmises ou matériellement mal transmises** aux utilisateurs,
(sigle **D**)

La documentation comprend la documentation technique relative aux matériels, les documents de navigation (cartes et documents terrains), les documents administratifs, etc.

Les informations, qui constituent une documentation provisoire, concernent les modifications de matériels, de procédures, d'organisation, les incidents ou accidents identifiés, etc.

→ *Défauts matériels*
(sigle complémentaire **m**)

Documentation inexistante, mal présentée matériellement (photocopie défectueuse, taille ou volume incompatible avec une utilisation dans le poste, etc.).

Information non transmise (erreur de transmission, liste de destinataires incomplète ou erronée), mal présentée matériellement ou mal transmise (Fax défectueux, incomplet, etc.).

→ *Contenu erroné*

(sigle complémentaire **c**)

Les données fournies par la documentation conduisent à des erreurs quant aux modèles utilisés pour la saisie des données, les décisions, la transmission des informations et les actions sur les commandes.

La documentation est rédigée par les concepteurs et non adaptée aux besoins de l'utilisateur qui n'y trouve pas ce qu'il y cherche.

Quelquefois les opérateurs utilisent une documentation "sauvage" (carnet personnel dont le contenu est incontrôlable).

Les informations fournies contiennent des erreurs (codes de référence incomplets ou contenant des fautes de frappes, schémas faux, incomplets ou périmés, etc.).

D'après PEYO

Exemple de mauvaise conception de la documentation.

⇨ **Réglementation inadaptée** (sigle **R**).

L'évolution des techniques, des méthodes d'utilisation des matériels peuvent rendre caduques et même néfastes des règles qui se sont montrées longtemps utiles et efficaces. Ce type d'erreur apparaît surtout lorsque les règlements ont été rédigés en imposant des moyens plutôt que des objectifs de sécurité.

⇨ Enfin, une dernière ligne a été crée portant le sigle **Z** pour couvrir les cas qui n'entreraient dans aucune des rubriques précédentes, dans la mesure où nul ne peut prétendre à l'exhaustivité. Bien entendu, un défaut ne peut être classé dans cette dernière ligne qu'avec des justifications appropriées et une révision du répertoire doit être proposée pour couvrir les cas analogues.

RÉPERTOIRE D'ANALYSE DES DÉFAUTS OPÉRATIONNELS DU SYSTÈME

RADOS

	Opérations d'exécution de la tâche au cours de laquelle est survenue l'erreur induite par le défaut système			
TYPE DE DÉFAUT SYSTÈME ⇩	Saisie et traitement de l'information **s**	Décision après traitement de l'information **d**	Transmission de l'information **t**	Action après décision **a**
	Homme ⇩ hh Homme / Machine ⇩ mh Homme		Homme ⇩ hh Homme / Homme ⇩ hm Machine	
ORGANISATION **Or** Qui doit faire ? (responsabilité)	Ors	Ord	Ort	Ora
ORGANISATION **Oe** Que doit-on faire ? (exécution)	Oes	Oed	Oet	Oea
ORGANISATION **Om** Quels moyens pour faire ? (moyens)	Oms	Omd	Omt	Oma
ORGANISATION **Op** Comment doit-on faire ? (procédures)	Ops	Opd	Opt	Opa
CONCEPTION de BASE **Hb** Conception reposant sur des hypothèses douteuses ou des principes inadaptés	Hbs	Hbd	Hbt	Hba
CONCEPTION des INTERFACES **Hm** Mauvaise ergonomie mécanique des interfaces	Hms	Hmd	Hmt	Hma
CONCEPTION des INTERFACES **Hc** Mauvaise conception des interfaces (ergonomie mentale)	Hcs	Hcd	Hct	Hca
FORMATION **Fb** Formation de base insuffisante	Fbs	Fbd	Fbt	Fba
FORMATION **Fs** Formation spécifique insuffisante	Fss	Fsd	Fst	Fsa
DOCUMENTATION **Dm** Défauts matériels	Dms	Dmd	Dmt	Dma
DOCUMENTATION **Dc** Contenu défectueux Documentation "sauvage"	Dcs	Dcd	Dct	Dca
RÉGLEMENTATION **R**	Rs	Rd	Rt	Ra

EXEMPLES ILLUSTRANT L'UTILISATION DE LA GRILLE RADOS.

⇨ COLONNE (s) Saisie et traitement de l'information

→ ORGANISATION (Qui doit faire ?) (Ors)

→ L'opérateur ne relève pas les informations qu'il doit normalement surveiller car il pense que cette tâche incombe à un autre. Au cours d'une opération de maintenance il constate une anomalie (des coffres sont restés ouverts par exemple), mais ne le signale pas pensant que ce n'est pas à lui de la faire (pas dans ses attributions) et que d'autres s'en chargeront normalement.

→ Au cours d'une opération de chargement, l'un des opérateurs, responsable de la surveillance du déplacement des charges, ne s'occupe que d'un secteur géographique restreint pensant que les autres secteurs sont surveillés par d'autres opérateurs.

→ Au cours d'une opération d'accostage du navire un observateur à la passerelle constate la présence d'un obstacle imprévu et ne le signale pas au responsable de la manœuvre pensant que ce n'est pas de son ressort.

→ ORGANISATION (Que doit-on faire ?) (Oes)

→ L'opérateur ne connaissant pas les limites de la tâche à effectuer relève simplement quelques informations partielles et ne saisit pas les informations dont il ignore l'importance.

→ ORGANISATION (Quels moyens pour faire ?) (Oms)

→ L'opérateur ne relève pas correctement une information car le moyen de mesure mis à sa disposition est inadapté (précision, échelle trop grande, etc.)

→ L'opérateur ne dispose pas du personnel qualifié pour effectuer une mesure ou lire une information.

→ L'opérateur ne dispose pas du nombre de personnels suffisant pour surveiller le déplacement d'une charge au cours d'une opération de manutention.

→ ORGANISATION (Comment doit-on faire) (Ops)

→ La procédure mise à la disposition de l'opérateur ne précise pas sur quel instrument relever une information alors que plusieurs afficheurs fournissent la même information mais avec des précisions différentes.

→ CONCEPTION de BASE (Hb)

Nous donnons ici des exemples de défauts de conception généraux sans qu'il soit possible de les affecter à l'une plutôt qu'à l'autre des colonnes de la grille.

→ La structure a été conçue en ne tenant pas compte de phénomènes physiques dangereux dans certaines conditions de fonctionnement (phénomènes de fatigue ou de flottement des structures par exemple).

- Exemple du Comet dont la structure avait été conçue sans tenir compte du phénomène de fatigue du fuselage due aux contraintes alternées produites par la pressurisation de la cabine passagers, phénomène mal connu à l'époque.

→ La logique de fonctionnement d'un automatisme ne tient pas compte de certaines circonstances, rares mais possibles, ce qui conduit à des réponses aberrantes de l'automatisme ou à une mise hors service intempestive.

- Exemple de l'accident d'ARIANE V. Un logiciel de surveillance de la dérive latérale au départ de la fusée a commandé la remise à zéro des centrales à inertie provoquant des ordres abusifs de corrections de trajectoires aboutissant à la rupture de la structure. Ce logiciel, parfait pour ARIANE IV a été utilisé tel quel sur ARIANE V, alors que le domaine possible de dérive latérale au décollage était différent.
- Exemple de quelques pilotes automatiques des avions de l'avant dernière génération. Le mode de base du pilote automatique en montée était un mode assurant une vitesse verticale constante. Ce mode était mis en service automatiquement en cas de défaillance du mode en service, sans que l'équipage en soit clairement prévenu. Or à haute altitude, le maintien de la vitesse verticale conduit à une réduction de la vitesse aérodynamique (les moteurs, pleins gaz, ne peuvent assurer la performance de montée). La réduction de vitesse pouvait alors se poursuivre jusqu'au décrochage aérodynamique, c'est-à-dire à la perte de contrôle de l'avion (voir au chapitre 7 l'exemple de l'accident du DC10 d'Aéromexico)

→ La conception de base peut reposer sur des hypothèses fausses de fréquence d'apparition des pannes, ce qui conduit, en service, à des défaillances graves des systèmes avec pertes de fonctions utiles à la sécurité.

→ Les seuils d'apparition d'alarme sont trop près des limites et ne laissent pas aux opérateurs le temps de réagir pour ramener la machine dans le domaine opérationnel.

→ CONCEPTION des INTERFACES (Hms)

→ Un capteur défectueux transmet une valeur erronée à un instrument d'un panneau de surveillance.

→ Une clé dynamométrique mal étalonnée indique une valeur d'effort erronée.

→ Un instrument mal éclairé dont l'aiguille grise se déplace sur fond gris avec des graduations blanches délavées conduit à une erreur de lecture.

→ La signalisation est "masquée" par le soleil.

→ Étiquetage défectueux du système sur lequel doit se dérouler une opération de maintenance (étiquette manquante, masquée partiellement par de la graisse, local mal éclairé)**.**

→ La procédure écrite fournie à l'opérateur comporte une erreur matérielle (ligne manquante en bas de page par suite d'une mauvaise photocopie, pages interverties, erreur de frappe, etc.)

→ CONCEPTION des INTERFACES (Hcs)

→ Numérotation défectueuse ou ambiguë des organes à identifier.

→ Numérotation anarchique des organes et des instruments.

→ Les synoptiques ne sont pas orientés comme sur le "terrain" alors que l'opérateur peut voir simultanément le synoptique et le terrain.

→ La disposition des instruments sur le panneau est en contradiction avec la disposition spatiale des points de mesure sur le système réel ou sur le schéma de conduite

→ Un cas particulièrement pervers est celui de la signalisation en relation non biunivoque avec le phénomène à signaler. Par exemple, on ne transmet pas la position réelle d'un organe à l'aide d'un capteur approprié mais un paramètre plus ou moins en relation avec cette position. Par exemple, ordre d'un système automatique de changement de position (en général l'ordre est suivi d'effet sauf s'il y a panne de l'actionneur, alors indécelable par l'opérateur).

- Exemple industrie nucléaire

  Catastrophe nucléaire de Harrisburg (Three Mile Island). Ce n'était pas la position fermée de la vanne de décharge du circuit primaire qui était signalée mais l'ordre de fermeture.

- Exemple RATP

  Si le verrou du frein d'immobilisation reste bloqué mécaniquement, la signalisation indique que le frein est desserré, alors que le frein est serré.

- Exemple transport aérien.

  Sur le DC10 accidenté à Ermenonville (Chapitre 7), la signalisation, au tableau de bord, du verrouillage de la porte de soute était liée, non pas à la mise en place du verrou mais à la position de la poignée de fermeture.

→ FORMATION de BASE (Fbs)

→ La formation de base n'a pas suffisamment insisté sur la nature, l'ordre de grandeur, l'importance des paramètres nécessaires au contrôle du processus.

→ FORMATION SPECIFIQUE (Fss)

→ La formation spécifique n'a pas suffisamment insisté sur la disposition des instruments de mesure (d'où une erreur de localisation de la source d'information), sur les particularités des échelles de mesure (zéro, échelle, sens de variation, etc.. d'où une erreur sur le modèle de transposition de l'information), sur les moyens d'identification des sources d'information, etc.

→ L'entraînement a été effectué sur un système différent du système réel (simulateur par exemple) avec une disposition non conforme des instruments sur le pupitre.

→ DOCUMENTATION (Dcs)

→ La documentation sur les sources d'information est difficilement compréhensible ou trop dispersée et conduit à des erreurs de saisie de données. Par exemple, il n'est pas clairement précisé que les étendues de mesure des instruments donnant les valeurs de plusieurs paramètres analogues ne sont pas identiques (zéros et échelles différentes).

→ Les schémas fournis sont des schémas de conception et non des schémas d'utilisation, les organes ne sont pas disposés sur le schéma comme sur le "terrain".

→ Les schémas fournis sont des reproductions en noir et blanc de schémas en couleurs et l'identification des sources d'information fait appel à la couleur.

→ Une modification des sources d'information n'est pas signalée (Dms) ou signalée avec erreurs (Dcs) aux opérateurs (panne de capteur, changement de type d'instrument avec par exemple changement d'échelle, déplacement des instruments sur le tableau de bord avec par exemple interversion de deux instruments mesurant des paramètres de même nature, changement de fréquence d'une balise, etc.)

.→ REGLEMENTATION (Rs)

→ La réglementation impose des signalisations de sécurité qui surchargent inutilement l'opérateur (panneaux multiples d'avertissement de travaux sur la voie).

→ La réglementation impose des types d'instruments d'une technologie dépassée.

⇨ COLONNE (d) Décision après traitement de l'information

→ ORGANISATION (Qui doit faire ?) (Ord)

→ Une décision est prise par un opérateur qui n'a pas les qualifications nécessaires ou le niveau hiérarchique prévu et qui, par suite, n'a pas accès aux informations adéquates permettant cette décision.

Par exemple, un opérateur constate une anomalie, mais ne se sentant pas responsable ne la signale pas à son supérieur pensant que c'est à lui de réagir. Au contraire il décide d'intervenir de sa propre initiative sans signaler au bon niveau de décision l'intervention en cours.

→ Une décision est prise par un responsable de haut niveau qui ne dispose pas des informations appropriées.

→ Un incident survient alors qu'un opérateur de maintenance fait un accompagnement en ligne sur une rame RATP. Il prend sur lui de faire le dépannage sur place, alors que l'objectif des exploitants est de dégager le train le plus rapidement possible.

→ ORGANISATION (Que doit-on faire ?) (Oed)

→ L'organisation n'a pas prévu les actions à entreprendre dans des situations particulières, rares, mais prévisibles.

→ ORGANISATION (Quels moyens pour faire ?) (Omd)

→ L'opérateur ne dispose pas des moyens matériels nécessaires ou adaptés à sa prise de décision (abaques ou schémas incomplets ou peu précis par exemple). Ce cas est quelque fois difficile à distinguer du cas suivant (Opd), des problèmes d'interface (Hmd et Hcd) ou des problèmes de documentation (Dmd et Dcd)

→ ORGANISATION (Comment doit-on faire ?) (Opd)

→ Les procédures de décision ne sont pas adaptées ou ne sont pas précisées.

→ Les procédures de décision sont ambiguës ou difficiles à interpréter (en particulier interdiction sur critères négatifs du style "il n'est pas interdit de ne pas ouvrir le robinet si le réservoir n'est pas plein").

→ La procédure prévoit des vérifications avant enclenchement de la suite des opérations (points d'arrêt), mais ne précise pas ce qu'il convient de faire si les vérifications ne sont pas acquises. Par exemple la procédure prévoit, avant intervention sur un circuit, de vérifier qu'il est bien hors tension. Cette recommandation est judicieuse, encore faut-il préciser ce que doit faire l'opérateur s'il constate que le circuit est toujours sous tension, "ouvrir le disjoncteur D312"," en référer à la hiérarchie (comment et dans quels délais)"," attendre (combien de temps)", etc. Il est clair que laissé à sa propre initiative, l'opérateur peut sortir du domaine de sécurité prévu pour l'intervention, dès lors que les limites, techniques et fonctions du temps, peuvent dépendre d'événements indépendants du seul opérateur.

→ CONCEPTION de BASE (Hb)

voir les exemples donnés pour la colonne **s** saisie des informations.

→ CONCEPTION des INTERFACES (Hmd) et (Hcd)

Ce type d'erreur est généralement rare, une mauvaise décision provenant le plus souvent, dans le cas d'une erreur d'interface, d'une mauvaise information. On peut néanmoins citer les quelques éventualités suivantes.

- → Une erreur matérielle dans la présentation d'un schéma de décision sur écran induit une mauvaise décision de la part de l'opérateur (Hmd).
- → Une erreur de logiciel d'aide à la décision induit une mauvaise décision de la part de l'opérateur (Hmd).
- → Le cahier des charges de rédaction du logiciel d'aide à la décision n'a pas prévu le cas particulier dans lequel se trouve l'opérateur face à son système ce qui amène ce dernier à une erreur de diagnostic donc de décision (Hcd).
- → Un synoptique d'aide à la décision, par une mauvaise présentation (par exemple arbre de décision trop "touffu") ou par des questions mal posées (par exemple avec des doubles négations), peut conduire à une erreur de décision (Hcd).
- → Une formulation ambiguë peut conduire à l'erreur, par exemple "si la condition A n'est pas réalisée, non-interdiction de passer la pompe en grande vitesse" (Hcd).
- → Une information touffue, difficile à synthétiser peut conduire à une erreur de décision (Hcd).

→ FORMATION de BASE (Fbd)

- → La formation de base a présenté des modèles de principe de fonctionnement du système incompris par les opérateurs (par exemple, l'opérateur croit que la relation pression - température est la loi des gaz parfaits de Mariotte alors que c'est la loi de vapeur saturante qui est en cause).

→ FORMATION SPECIFIQUE (Fsd)

- → La formation spécifique fournit des modèles trop généraux de fonctionnement du système, modèles qui ne sont pas applicables dans quelques cas particuliers. Dans ces cas là, les opérateurs font reposer leurs décisions sur le principe général non applicable.
- → L'entraînement a été effectué sur un système différent du système réel (simulateur par exemple) avec des modes de fonctionnement simplifiés non conformes aux modes de fonctionnement réels.

→ DOCUMENTATION (Dmd)

- → La documentation sur les modèles de fonctionnement permettant les décisions est inexistante, incomplète, mal reproduite, difficilement maniable sur le terrain (organigrammes de grandes dimensions ou manuels multiples inutilisables en extérieur) ou encore contient des erreurs matérielles (fautes de frappe sur des codes d'identification d'organes par exemple).
- → Une modification des règles et consignes de conduite, de l'organisation (répartition des tâches par exemple) n'est pas transmise.
- → Une information d'interdiction de survol n'a pas été transmise ce qui conduit l'équipage à une mauvaise décision sur la trajectoire à suivre.

→ DOCUMENTATION (Dcd)

- → La documentation sur les modèles de fonctionnement permettant les décisions est difficilement compréhensible, ou trop dispersée, et conduit à des erreurs de décision. Par exemple, les organigrammes de décision comportent des ambiguïtés ou encore ne présentent que le modèle de fonctionnement général du système, et renvoient les cas particuliers à des annexes sans en signaler l'importance sur le plan sécurité.
- → Une modification des règles et consignes de conduite, de l'organisation (répartition des tâches par exemple) est transmise avec erreurs aux opérateurs.

→ REGLEMENTATION (Rd)

- → La réglementation impose des accords multiples de la hiérarchie retardant la prise de décision dans des cas d'urgence.

⇨ COLONNE (t) Transmission de l'information

→ ORGANISATION (Qui doit faire ?) (Ort)
- → L'organisation n'a pas prévu la liste complète des émetteurs et des destinataires des messages dans tous les cas possibles. Par exemple, en situation de maintenance lorsqu'une impossibilité de poursuivre apparaît, qui prévenir et quelle information transmettre ?

→ ORGANISATION (Que doit-on faire ?) (Oet)
- → L'organisation n'a pas prévu la liste systématique des moyens de transmission des messages et des méthodes d'utilisation des moyens de transmission, en couvrant tous les cas possibles de fonctionnement normal et d'incidents des systèmes de transmission. Par exemple, en cas de panne d'interphone que dois-je faire en fonction de l'urgence et du type de destinataire ?

→ ORGANISATION (Quels moyens pour faire ?) (Omt)
- → L'opérateur ne dispose pas des personnels nécessaires ou adaptés à la transmission des informations (personnel non qualifié en particulier).
- → L'organisation n'a pas prévu que les moyens de transmission des messages ne sont pas disponibles là où se trouve l'opérateur (absence de téléphone par exemple).

→ ORGANISATION (Comment doit-on faire ?) (Opt)
- → Quelquefois l'opérateur est obligé de mémoriser un certain nombre de valeurs pendant un temps plus ou moins long (cas de transmission de l'opérateur vers lui-même). Cette opération de mémorisation comporte des risques d'erreurs ou d'oubli. L'organisation a-t-elle prévu des moyens simples de stockage provisoire de l'information (ardoise, papier, planchette, tableau "gras", système d'affichage mécanique ou électronique, etc.).
- → L'organisation n'a pas prévu de procédures simples d'émission des messages d'urgence (numéros d'appel banalisés des services d'urgence à rechercher dans l'annuaire général par exemple).

→ CONCEPTION de BASE (Hb)

voir les exemples donnés pour la colonne **s** saisie des informations.

→ CONCEPTION des INTERFACES (Hmt)
- → Le système de transmission de l'information est dégradé, par exemple par panne ou insuffisance mécanique, électrique ou électronique, par brouillage ou bruitage (ambiance sonore élevée) ou par mauvaise visibilité (éclairage non nominal, brouillard,...).
- → Les claviers de commande des moyens de transmission sont inadaptés à la manipulation (touches trop petites, pas assez espacées, le pupitre est trop éloigné de l'opérateur, etc.)

→ CONCEPTION des INTERFACES (Hct)
- → Le système de transmission ne permet pas d'identifier facilement le canal de transmission (affichage de fréquence prêtant à confusion) ou d'identifier clairement le destinataire des messages.
- → Les claviers de commande de transmission facilitent les confusions, panneau carrés de cent touches de formes et de couleurs identiques, choix du destinataire (interphone, émission radio) fait par un inverseur indépendant du bouton poussoir d'émission, etc.

→ FORMATION de BASE (Fbt)
- → La formation de base n'a pas suffisamment insisté sur les règles et les procédures générales de transmission de l'information, nécessité de s'identifier clairement en tant qu'émetteur, nécessité de préciser le destinataire, nécessité d'utilisation de format précis de message (code alphabétique par exemple), etc.
- → La formation de base n'a pas suffisamment insisté sur l'organisation de l'entreprise et les règles de sécurité justifiant les besoins et les moyens de transmission d'information.

→ FORMATION SPECIFIQUE (Fst)
- → La formation spécifique n'a pas suffisamment insisté sur les moyens et méthodes de transmission de l'information et n'a pas justifié les procédures à utiliser.

→ L'entraînement a été effectué sur un système différent du système réel (simulateur par exemple) sans entraînement à la transmission des informations.

→ DOCUMENTATION (Dmt)
- → La documentation sur les moyens et les procédures de transmission est inexistante, incomplète, mal reproduite, difficilement maniable sur le terrain (listes multiples de destinataires ou de fréquences inutilisables en extérieur, caractères trop petits difficilement lisibles sous faible éclairage) ou encore contient des erreurs matérielles (oubli de mise à jour, fautes de frappe sur les codes, les noms de destinataires ou les fréquences par exemple).
- → Une modification des règles et consignes de transmission, une modification de l'organisation (changement des destinataires des messages), une modification d'un annuaire, n'est pas transmise aux opérateurs.

→ DOCUMENTATION (Dct)
- → La documentation sur les moyens et les procédures de transmission est difficilement compréhensible ou trop dispersée et conduit à des erreurs. Les annuaires ou les listes de fréquences comportent des ambiguïtés ou rendent difficile la recherche d'un code de correspondant.
- → Une modification des règles et consignes de transmission, une modification de l'organisation (changement des destinataires des messages), une modification d'un annuaire, est transmise avec erreurs aux opérateurs.

→ REGLEMENTATION (Rt)
- → La réglementation impose l'utilisation de types de messages lourds retardant d'autant la transmission d'information dans les cas d'urgence.

⇨ COLONNE (a) Action

→ ORGANISATION (Qui doit faire ?) (Ora)
- → L'opérateur n'exécute pas les actions prévues parce qu'il croit que c'est à un autre de les faire. C'est le problème de partage des tâches entre le mécanicien d'entretien et l'électricien (qui doit entretenir les capteurs ?).
- → L'opérateur entreprend des actions normalement dévolues à un autre ce qui peut provoquer des incompréhensions de part et d'autre tant que les opérateurs ne communiquent pas.

→ ORGANISATION (Que doit-on faire ?) (Oea)
- → L'organisation n'a pas prévu la liste systématique des actions et des procédures à suivre, en couvrant tous les cas possibles de fonctionnement normal et incidentels des systèmes. Par exemple, a-t-on prévu quelle procédure suivre, ou quitter, en cas d'impossibilité de poursuivre une opération de maintenance ?

→ ORGANISATION (Quels moyens pour faire ?) (Oma)
- → L'opérateur ne dispose pas des moyens en personnel pour exécuter toutes les actions dans le temps qui lui est imparti pour accomplir la tâche.
- → L'opérateur ne dispose pas des moyens matériels (outillage, engins de chantier, matériel de levage, etc.) adaptés à l'exécution de la tâche.

→ ORGANISATION (Comment doit-on faire ?) (Opa)
- → C'est dans cette catégorie qu'entrent le non-respect des procédures établies et le recours aux procédures "exotiques" du style "tu vas voir, j'ai ça dans mon calepin". L'analyse nécessite alors de se poser la question "Pourquoi la procédure prévue n'a pas été suivie (impossibilité physique, manque de moyens en homme ou en matériel, mauvaise interprétation, procédure mal adaptée, adaptation de "règles de l'art" non appropriées, etc.) avant d'assimiler l'erreur à une faute contre la discipline.

  Ainsi, au cours des manœuvres de refoulement de trains coupés en atelier, la procédure réglementaire n'est pas respectée. Le shuntage de la boucle de sécurité n'est pas mis en place et le manipulateur en loge arrière est utilisé. La manœuvre n'en est pas modifiée, mais le frein de secours est inutilisable.

  C'est l'exemple dramatique et réel du pilote qui décide de parcourir la piste avec les réacteurs à fort régime et en freinant énergiquement, afin de chauffer l'atmosphère et ainsi dissiper temporairement le

brouillard. Il en est résulté une température anormale des freins qui a conduit à l'explosion des pneumatiques une fois le train rentré après le décollage et la destruction fatale des circuits hydrauliques.

→ CONCEPTION de BASE (Hb)

voir les exemples donnés pour la colonne **s** saisie des informations.

→ CONCEPTION des INTERFACES (Hma)

- → Les commandes ne sont pas adaptées à l'opérateur (touches trop petites, insuffisamment espacées, leviers de taille, forme, débattement rendant la manipulation mal commode ou fatigante, etc.).
- → Les commandes dont la manipulation peut conduire à des changements d'états irréversibles ou dangereux ne sont pas protégées par des caches en interdisant la manipulation intempestive (boutons d'arrêt d'urgence, signal d'évacuation immédiate des locaux, etc.)

→ CONCEPTION des INTERFACES (Hca)

- → Les commandes sont disposées suivant une logique sans rapport avec la disposition des organes commandés.
- → Les commandes ont un sens d'action inhabituel (robinet s'ouvrant dans le sens à visser, potentiomètre diminuant le volume d'amplification dans le sens à visser, etc.).
- → Les commandes ont un sens d'action sans relation avec l'effet sur l'organe commandé (un levier tiré vers le haut déplace la charge vers le bas, poussé à droite déplace la charge vers la gauche ou vers l'avant, etc.).
- → Un mauvais fonctionnement du système de commande rend une commande inefficace ou erronée; par exemple un bouton poussoir est appuyé, il s'allume pour signaler uniquement qu'il a été poussé, mais l'ordre n'a pas été transmis au système (effet pervers analogue à celui décrit en Hcs). L'opérateur est ainsi trompé par un faux retour d'information sur l'effet de la commande. Le même effet pervers peut être obtenu par une commande mécanique ou électrique débranchée; le levier ou l'interrupteur a été mis en bonne position mais l'ordre n'a pas été transmis.

→ FORMATION de BASE (Fba)

- → La formation de base n'a pas suffisamment insisté, au niveau des principes, sur l'influence, l'effet (sens et efficacité, effets parasites), des commandes sur le processus à contrôler.

  A titre d'exemple la présentation de la loi d'Ohm sous la forme $P = R.I^2$ fait croire qu'il faut augmenter la résistance d'une chaufferette (alimentée par le secteur à voltage constant) pour augmenter la puissance de chauffage, alors que la présentation sous la forme $P = V^2 /R$ démontre sans ambiguïté qu'il faut effectuer l'opération inverse.

→ FORMATION SPECIFIQUE (Fsa)

- → La formation spécifique n'a pas suffisamment insisté sur la disposition spatiale des commandes (d'où une erreur de localisation des commandes), sur les particularités des sens d'action des commandes, sur les moyens d'identification des commandes (formes, couleurs, étiquetage, etc.), sur les retours d'information d'état des organes commandés, etc.
- → L'entraînement a été effectué sur un système différent du système réel (simulateur par exemple) avec une disposition, des types de commandes non conformes aux commandes réelles sur le pupitre.

→ DOCUMENTATION (Dma)

- → La documentation sur les commandes est inexistante, incomplète, mal reproduite, difficilement maniable sur le terrain (plans de grandes dimensions ou manuels multiples) inutilisables en extérieur ou encore contient des erreurs matérielles (fautes de frappe sur des codes d'identification des commandes par exemple).
- → Une modification des commandes (position, forme, identification, sens d'action, etc.) n'est pas signalée aux opérateurs (panne, changement de type de commande avec, par exemple, changement de sens d'action, déplacement des commandes sur le tableau de bord avec, par exemple, interversion de deux commandes agissant de façon analogue sur le système, etc.).

→ DOCUMENTATION (Dca)

- → La documentation sur les commandes est difficilement compréhensible ou trop dispersée et conduit à des erreurs d'action. Par exemple, il n'est pas clairement précisé le sens d'action particulier d'une commande, ses effets parasites sur le contrôle du système.

→ Les schémas fournis sont des schémas de conception et non des schémas d'utilisation, les commandes ne sont pas disposées sur le schéma comme sur le poste de travail.

→ Une modification des commandes (position, forme, identification, sens d'action, etc.) est signalée avec des erreurs aux opérateurs (panne, changement de type de commande avec changement de sens d'action, par exemple, déplacement des commandes sur le tableau de bord avec interversion de deux commandes agissant de façon analogue sur le système, par exemple, etc.).

→ REGLEMENTATION (Ra)

→ La réglementation impose le verrouillage de certaines commandes interdisant leur utilisation en cas d'urgence.

GOOF

RAFT

GASP

GAME

GARE

GAFE a été traduit en anglais par GOOF (Grid Of Operator Failure d'où Goofy, personnage bien connu de Walt Disney)
et RADOS traduit par RAFT (Rapid Analysis Failures Table)(radeau).
"To make a Smurf gasp" signifie "couper le souffle à un Schtroumpf".

GRILLE DES FACTEURS AMPLIFICATEURS DE RISQUE D'ERREUR

⇨ Confort réduit
- sièges
- posture anormale
- local confiné, étroit
- travail dans l'espace

⇨ Tenue de travail gênante
- combinaison de sécurité (sécuracide, spatiale, etc.)
- gants, bottes, casque, lunettes, masque (antipoussière, oxygène), écouteurs, sourdines

⇨ Mouvements de plate-forme
- vibrations
- secousses
- oscillations lentes
- travail en impesanteur
- travail sous facteur de charge

⇨ Ambiance
- Températures extrêmes
- Pression anormale (travail en caisson pressurisé, à faible pression)
- Humidité
- Éclairage violent ou trop faible
- Bruits
- Odeurs

⇨ Horaire d'exécution de l'opération à l'instant de l'incident
- Début de mission, Fin de mission
- Reprise du service, remise en route des installations
  le matin, en début de semaine, après un jour chômé, après une période de congé annuel
- Arrêt du service, arrêt des installations
  le soir, en fin de semaine, avant un jour chômé, avant la période de congé annuel
- Opérations pendant le week end, un jour chômé, pendant la période de congé annuel
- Changement des équipes de quart
- Après un changement des horaires (systèmes de transports)

⇨ Tâches spéciales
- Entraînement sur système réel
- Entraînement sur simulateur
- Essai sur système réel
- Essai sur simulateur
- Mission non commerciale (convoyage, ..)

⇨ État du système à l'instant de l'incident
- Fonctions non assurées par la machine
- Capteurs, chaînes de transmission de données, afficheurs en panne
- Commandes, chaînes de commande, actionneurs en panne
- Chaînes de transmission, émetteurs, récepteurs en panne
- Systèmes, sous systèmes, automatismes en panne

⇨ **Facteurs internes. (**sigle **Pki)**
⇨ Utilisation de médicaments
⇨ Absorption d'alcool
⇨ Usage de drogues

⇨ **Facteurs physiologiques. (**sigle **Pg)**

- Douleurs (tête, dents, oreilles, yeux, dos, etc.)
- Douleurs gastriques, abdominales, musculaires, articulaires, etc.
- Démangeaisons
- Incapacitation (évanouissement, décès)
- etc.

⇨ **Facteurs psychologiques. (**sigle **Pz)**

⇨ Peur
⇨ Angoisse
⇨ Préoccupations personnelles
- heureuses (réussite amoureuse, promotion, gain au jeu, etc.)
- malheureuses (échec amoureux, réprimande, perte au jeu, problèmes de santé, etc.)

⇨ Préoccupations et soucis familiaux (maladie d'un membre de la famille, naissance prochaine, chômage du conjoint, d'un enfant, problèmes financiers, etc.)
⇨ État psychopathologique (perte de mémoire, "folie", etc.)

⇨ **Facteurs sociologiques. (**sigle **S)**

⇨ **Facteurs internes. (**sigle **Si)**

⇨ Composition de l'équipe ou de l'équipage
⇨ qualification des membres (ancienneté, connaissances) *
⇨ sous effectif occasionnel
⇨ présence de stagiaires
⇨ conflits internes à l'équipe

⇨ **Facteurs externes. (**sigle **Se)**

⇨ Climat social (grèves, manifestations)
⇨ Présence d'un visiteur
⇨ Présence d'un instructeur
⇨ Présence d'un examinateur
⇨ Présence d'une personnalité

On notera que parmi ces facteurs, certains sont directement dus à une mauvaise conception ergonomique du poste (confort, tenue de travail, ambiance), à des problèmes d'organisation (horaires, besoins physiologiques ou facteurs sociologiques) ou à des problèmes de conception de base (pannes de la machine). Il faut les signaler à ce stade d'observation car ils constituent des facteurs aggravant pouvant expliquer les erreurs observées, mais il faut également les noter parmi les défauts du système à corriger.

A la suite d'un accident, l'enquête permet généralement de retrouver la plus grande partie de ces facteurs. Par contre, dans bien des cas de simples incidents, il est difficile d'obtenir des renseignements suffisants pour déterminer les facteurs psychologiques et sociologiques internes.

* Voici quelques exemples de composition d'équipage entraînant des risques:
- Un officier brillant, mais jeune et sans grande expérience pratique et un vieux sous officier très pragmatique et peu soucieux des aspects théoriques.
- Un commandant de bord ancien et un tout jeune copilote, avec deux attitudes possibles du commandant,
  - bienveillant, il se préoccupe de la formation de son jeune collègue et en oublie de mener à bien sa propre tâche,
  - malveillant, il ne pense qu'à mettre en évidence les manques de son collègue et à s'en indigner.
- Équipage constitué de deux commandants de bord de même ancienneté.

GRILLE D'ANALYSE DES ÉVÉNEMENTS DE SENSIBILITÉ AUX PERTURBATIONS

GASP

Grille définie pour l'étude des incidents et accidents d'avions de transport civils

Perturbations externes	Sigle
rafale	Sraf
gradient de vent	Sgrv
turbulence	Stur
foudroiement	Sfdr
givrage	Sgiv
grêlons	Sgrl
variation brutale de l'état de la piste (trous, flaque d'eau, etc.)	Spst
oiseaux	Soix

Perturbations internes	Sigle
panne de système (il s'agit de la perturbation provoquée par l'apparition de la panne et non de l'effet de la panne établie)	Span
feu	Sfeu
perte de pressurisation	Sprs
perturbation commise par un passager	Spax

Ces grilles sont caractéristiques du système de transport civil aérien. Elles ne sont valables que dans ce cas.

GRILLE D'ANALYSE DES ÉVÉNEMENTS DE MANŒUVRABILITÉ

GAME

Grille définie pour l'étude des incidents et accidents d'avions de transport civils

Manœuvres correctives	Sigle
correction de vitesse ou de Mach	Mcm
correction d'incidence ou d'assiette longitudinale	Mci
correction de dérapage	Mcd
correction d'assiette latérale	Mca
correction de cap	Mcc
correction d'altitude	Mch

Manœuvres imposées par la mission	Sigle
changement de vitesse ou de Mach	Mmm
changement de pente (en particulier arrondi)	Mmp
changement de cap (mise en virage, virage, sortie de virage)	Mmc
changement d'altitude (mise en montée ou en descente, montée ou descente, mise en palier)	Mmh
changement de configuration (train, volets, etc.)	Mmf

Ces grilles sont caractéristiques du système de transport civil aérien. Elles ne sont valables que dans ce cas.

Retour d'Expérience sur le Retour d'Expérience !

Les notions de Facteur d'Erreur et d'Amplificateur de Risque.

L'utilisation des grilles pour l'analyse des incidents, en particulier les incidents de la base de donnée de l'ASRS*, nous a montré que la notion de Facteur d'Erreur n'était pas toujours bien comprise par les analystes. Il y a souvent confusion dans les esprits entre Facteur d'Erreur, Cause et Type d'Erreur.

Un Facteur d'Erreur, rappelons-le une fois de plus, définit les conditions au cours desquelles une erreur est commise, mais ne caractérise ni le type d'erreur commise, ni les causes de cette erreur. Par exemple une Charge de Travail élevée peut amener l'opérateur à ne pas remarquer la dérive d'un paramètre important, d'oublier d'exécuter une action nécessaire de correction, d'exécuter une autre action que celle nécessaire, de mettre trop de temps à l'exécuter, d'oublier de transmettre un message, etc. Mais le même Facteur d'Erreur peut ne conduire à aucune erreur. Mis dans la même situation, avec le même Facteur d'Erreur, par exemple au cours d'un exercice au simulateur reproduisant cette situation, deux opérateurs différents ou le même opérateur au cours de deux exercices différents, commettront des erreurs différentes. Ainsi les types d'erreur ne sont pas caractéristiques d'un Facteur d'Erreur.

Un Facteur d'Erreur définit la situation mentale de l'opérateur au moment où il commet une erreur.

Cette définition explique pourquoi nous avons mis dans la même grille GAFE, la Charge de Travail élevée, l'Absence de Stimuli, la Maladresse et les Erreurs de Représentation.

Montrons, à l'aide d'un modèle de fonctionnement très simpliste du cerveau, ce que nous appelons "situation mentale" de l'opérateur.

Dans le cas du premier Facteur d'Erreur, Charge de Travail élevée, le cerveau de l'opérateur n'a pas assez de neurones disponibles pour exécuter la tâche requise. Dans le second cas, Absence de Stimuli, les neurones sont "déconnectés"de l'évolution de la tâche à surveiller et "connectés" sur une tâche étrangère, souvenir du dernier film, de la dernière partie de campagne, du bricolage en cours,... Pour le dernier Facteur, la Maladresse, les neurones de l'opérateur ne sont pas correctement connectés, ce qui conduit à une mauvaise exécution de l'opération prévue, recueil d'information, action sur une commande, nature du message oral, etc. Dans ce cas de Maladresse, il est souvent difficile de préciser pourquoi et comment les neurones sont mal connectés, sauf, quelquefois, dans le cas d'une fausse manœuvre quand l'opérateur réagit instinctivement sans noter les obstacles dans son environnement ou dans le cas du message erroné quand l'opérateur utilise le mauvais mot parce qu'il vient juste d'entendre ce dernier. Enfin dans le cas des Erreurs de Représentation, la fausse image conduit à des connexions inadéquates des neurones.

Ne donnons pas à ce modèle du cerveau plus de valeur qu'il n'en a, c'est-à-dire aucune ! Il ne représente qu'une image commode pour illustrer notre propos.

Au cours d'une analyse d'un accident ou d'un incident, il est très important de ne pas s'en tenir au niveau de la grille GAFE des Facteurs d'Erreur, mais d'essayer d'expliquer la présence de ces Facteurs d'Erreur en examinant la grille RADOS. Les cinq articles de cette grille donnent une origine possible des Facteurs d'Erreur. Nous préférons utiliser le terme "origine" plutôt que "cause", parce que l'identification des causes profondes d'une erreur relève du travail du psychologue et non de celui du technicien. L'identification des origines d'un Facteur d'Erreur, plutôt que de ses causes, est suffisante pour l'objectif poursuivi par le technicien de la sécurité, à savoir définir les modifications à apporter au Système pour améliorer la sécurité.

D'un autre côté, nous pensons que les psychologues doivent maintenir la grille GAFE telle quelle, parce qu'elle aide à préciser la situation mentale de l'opérateur au cours de chacun des événements conduisant à un accident. Mais les psychologues doivent compléter cette grille par une autre grille, parallèle à la grille RADOS, montrant la relation entre les Facteurs d'Erreur et les erreurs elles-mêmes. Ce travail est très important mais il dépasse les compétences des techniciens !

Nous avons également observé, lors de nos études avec la NASA, la tentation, pour les analystes en formation, à mélanger les articles de la GARE avec ceux de la GAFE, c'est-à-dire à confondre les Facteurs d'Erreur avec les Amplificateurs de Risque.

* La base ASRS est un recueil, sous la responsabilité de la NASA, d'environ 80 000 rapports volontaires d'incidents survenus dans le domaine du transport aérien. Elle est gérée par la société Batelle.

Or il y a une grande différence entre ces deux notions. Un Facteur d'Erreur caractérise une situation mentale temporaire de l'opérateur. Un Amplificateur de Risque est plus permanent et est présent dans un certain nombre d'événements. Un Amplificateur de Risque, par exemple la fatigue ou une préoccupation d'ordre sociologique, accroît le désordre mental lorsque celui-ci est déjà présent. Par exemple, en utilisant notre modèle simpliste du cerveau, la fatigue réduit le nombre de neurones disponibles pour faire face à une charge de travail donnée ou augmente le nombre de mauvaises connexions conduisant à la maladresse. Des préoccupations réduisent les chances de détecter une fausse image de la situation opérationnelle. Mais nous devons noter que la fatigue est sans effet si aucun Facteur d'Erreur n'est présent. Fatigué ou non, un opérateur ne commettra pas d'erreur s'il n'a rien à faire ! Ainsi les Amplificateurs de Risque ne sont-ils jamais seuls à l'origine d'un accident, sauf peut-être dans les cas, peu fréquents, où l'opérateur est totalement hors circuit, mort ou évanoui.

Il est néanmoins important, au cours d'une analyse, d'identifier les Amplificateurs de Risque.

Répétons ce que nous avons déjà dit sur ce sujet. L'ensemble des Amplificateurs de Risque, présents dans un incident ou un accident, donne une idée de la probabilité d'observer le même type de situation dans d'autres cas. A titre d'exemple déjà cité, une erreur est commise par Charge de Travail trop élevée, avec un équipage très fatigué, une météo exécrable (turbulence, grêle, éclairs,..), un pilote dont l'épouse est sur le point d'accoucher, un copilote en cours de divorce et en présence du président de la compagnie dans le cockpit ! Il n'est sans doute pas nécessaire d'envisager une modification coûteuse du cockpit pour réduire la charge de travail dans une situation analogue.

Par contre les Amplificateurs de Risque ont généralement une origine qui peut être identifiée par un article de la grille RADOS. Les défauts du système ainsi identifiés doivent alors être pris en compte au même titre que les défauts à l'origine des Facteurs d'Erreur.

La notion d'Erreur de Représentation.

Cette notion abondamment développée jusqu'ici n'est peut-être pas bien caractérisée par ce terme d'"Erreur de Représentation". Ce terme, consacré maintenant par l'usage, pourrait être remplacé par "Mauvais État Mental", "Mauvaise Configuration Mentale", "Confusion Mentale", "Conscience erronée de la Situation" pour éviter le mot "erreur", car nous avons tendance à confondre l'état mental de l'opérateur et l'erreur elle-même commise (il y a erreur de représentation sur le terme "erreur de représentation" !). Nous avons ainsi connu de nombreuses difficultés à expliciter le concept auprès de nos interlocuteurs de la NASA, la langue et la démarche intellectuelle de type Anglo-Saxon, pragmatique et non cartésienne, ajoutant à la confusion !

Essayons de préciser le concept, sans changer le terme.

Lorsque l'opérateur prend une décision, lorsqu'il capte des informations, lorsqu'il transmet un message, lorsqu'il agit sur une commande ou lorsque qu'il ne fait rien et attend, il utilise quatre types de représentations mentales,

1/ des images du "monde" qui peuvent être divisées en deux types principaux,

1a/ images du monde extérieur au système, par exemple
- positions des autres avions, position des obstacles, météorologie.., pour un pilote d'avion,
- situation de la demande en énergie sur le réseau, énergie externe disponible en cas de panne, météorologie (glaces entravant la réfrigération..),.. pour l'opérateur d'une centrale nucléaire,
- situation des stockages extérieurs pour un opérateur d'une entreprise de production,
- situation, disponibilité des entités destinées à dialoguer au cours de la mission, situation, disponibilité du réseau de transmission

1b/ images du monde intérieur au système, par exemple
- configuration de l'avion, couvrant non seulement la configuration géométrique, trains et volets, mais également l'état des systèmes (moteurs, circuit de combustible, automatismes,..) (marche, arrêt, en panne partielle ou total),
- état du cœur du réacteur (pleine puissance, réduit, arrêt à chaud, arrêt à froid,..), de l'étage de fourniture d'énergie, des systèmes de sécurité, des auxiliaires,.. pour une centrale nucléaire.

- état des machines de production, état des systèmes de transport internes,.. pour une usine de production.

2/ des modèles de fonctionnement des systèmes qui représentent comment chaque système travaille en situation normale, en situation de panne partielle ou totale et qui permettent d'identifier les pannes de système.

Il faut prendre garde à ne pas confondre ces modèles avec les images d'état des systèmes décrits en 1b ou avec les images du système de transmission décrit en 1a.

Une image d'état d'un système définit si le système est sur Marche, sur Arrêt, s'il est partiellement ou totalement en panne. Un modèle de système définit comment fonctionne théoriquement un système. Bien entendu le modèle de fonctionnement du système, choisit par l'opérateur, peut dépendre de l'état du système et donc de son image d'état. Par exemple l'opérateur n'utilisera pas le même modèle de fonctionnement du cœur (et donc le même modèle de pilotage), suivant que le réacteur est à pleine puissance ou en arrêt à chaud.

De même un opérateur n'utilisera pas le même modèle d'organisation des transmissions avec les organismes extérieurs suivant que l'image qu'il se fait de l'état du système de transmission est celle d'un système intègre ou celle d'un système partiellement en panne (utilisation de procédures d'urgence simplifiées par exemple si le système de transmission est passé en situation secours).

Attention ! Le choix d'un mauvais modèle de fonctionnement peut provenir d'une ignorance de l'opérateur qui utilise le même modèle de fonctionnement quel que soit l'état réel du système ou d'une erreur sur l'identification de l'état du système qui lui fait choisir le modèle adapté à la situation perçue et non le modèle adapté à la situation réelle.

Ces modèles peuvent être très simplifiés ou trop simplifiés et par suite inadaptés à quelques situations exceptionnelles. Ils peuvent être plus complexes avec le risque de mauvaise utilisation par difficulté d'application dans des cas particuliers.

- **3/** les modèles d'interface opérateurs – machine, qui permettent le dialogue homme – machine.

Ces modèles comportent
- les modèles de localisation des instruments
- les modèles d'identification des instruments
- les modèles de transposition de l'information
- les modèles de localisation des commandes
- les modèles d'identification des commandes
- les modèles de mode d'action des commandes
- les modèles de retour d'information sur les positions de commande

Il faut y ajouter tous les modèles analogues utilisés pour les transmissions d'information.

- **4/** le "Modèle de Tâches" qui lui permet de définir l'objectif de la sous phase en cours d'exécution

- **5/** le "Modèle de Risque" qui aide l'opérateur à estimer le danger lié à l'état de sa machine, état externe et état interne et au résultat envisagé des opérations qu'il a décidé d'exécuter.

Par exemple le temps est calme, l'avion est en croisière haute altitude et tous les systèmes fonctionnent normalement. Le pilote estime alors que le risque est très faible. Le temps est exécrable, neige, givrage et turbulences fortes, l'avion est en phase d'approche à basse altitude, un moteur en panne, sur un terrain de montagne et le trafic aérien est intense. Le pilote estime, avec juste raison, que le risque est élevé et qu'il faut éviter toute manœuvre intempestive.

Lorsque l'opérateur utilise une mauvaise représentation mentale, il prend généralement de mauvaises décisions. Les conséquences de ces décisions sont d'une autre nature que les conséquences d'erreurs dues à une charge de travail trop élevée, à une absence de stimuli ou à une maladresse. En cas d'erreur de représentation il y a en général un délai avant la catastrophe. Par exemple, suite à une charge de travail trop élevée, le pilote ne voit pas que l'altitude est trop basse compte tenu du relief. L'impact avec le sol ne va pas tarder. Dans une autre situation le pilote s'imagine que l'avion est au Nord du terrain alors qu'il est en réalité au Sud. Cette situation n'est que potentiellement dangereuse et ne conduit à la catastrophe que si le pilote décide de descendre sur le Sud montagneux.

L'opérateur d'une centrale nucléaire s'imagine que les systèmes de sécurité sont disponibles alors qu'une panne, non perçue les a mis hors service. Tant que le fonctionnement du cœur sera nominal, ne nécessitant pas la mise en service des sécurités, la situation ne sera que potentiellement dangereuse.

Les origines de ces Consciences erronées de la situation sont très nombreuses. Sans prétendre à l'exhaustivité nous pouvons citer les quelques exemples suivants qui complètent ceux déjà donné.

A/ En raison d'une charge de travail élevée, d'une absence de stimuli du fait que la situation est stationnaire depuis un long moment, le pilote ne remarque pas la panne d'un système, la proximité d'un autre avion, le survol d'un "way point"*,..

A la suite d'une maladresse, un interrupteur a été mis en position "arrêt" et cet événement n'a pas été remarqué.

La conséquence de ces événements est une fausse image mentale extérieure au système (le pilote ignore le danger dû à la présence d'un autre avion ou il pense que le "waypoint" est encore devant l'avion) ou la conséquence en est une fausse image intérieure (le pilote pense que le système en panne ou que le système mis sur "arrêt" est toujours en service et il l'utilise). La probabilité de se trouver dans ce type de situation est augmentée en cas de fatigue de l'équipage, de souci ou de conflit social (GARE).

B/ L'opérateur fait une lecture erronée d'un paramètre (problèmes d'éclairage ou de visibilité). Par exemple il lit une pression de 50 bars au lieu de 40 bars sur un manomètre, il lit une température de 60°C au lieu de 80°C sur un thermomètre.

En raison de la mauvaise fidélité d'un haut-parleur, l'opérateur interprète à tort un message oral d'un autre opérateur ("vanne six fermée" alors que le message est "vanne dix fermée").

L'opérateur actionne la mauvaise touche d'un clavier trop petit. Il tape 106 au lieu de 109 par confusion entre la seconde et la troisième ligne du clavier (confusion classique conduisant à taper un mauvais numéro de téléphone).

Ces erreurs proviennent généralement d'une mauvaise conception du tableau de bord (RADOS).

Toutes ces erreurs ont pour conséquence une mauvaise image de la situation du système.

C/ L'opérateur relève une donnée sur le mauvais instrument (modèle de localisation des sources d'information). Par exemple il relève la température de la turbine 3 au lieu de la température de la turbine 2.

Le paramètre affiché sur un instrument dépend de la position d'un commutateur, ce qui conduit par exemple le pilote à lire une vitesse verticale au lieu d'un angle de pente (modèle d'identification des instruments).

La couleur ambre d'un paramètre affiché sur un écran de contrôle est vue comme rouge et interprétée comme une alarme. La position de l'aiguille d'un instrument est interprétée comme indiquant une valeur autorisée parce que l'opérateur n'utilise pas la bonne échelle de mesure sur un instrument comportant plusieurs échelles, le choix de l'échelle étant choisi par un commutateur situé loin de l'instrument (modèles de transposition de l'information).

D/ L'opérateur n'actionne pas le sélecteur adéquat, mettant ainsi en service un automatisme non désiré (modèle de localisation des commandes).

L'opérateur met un sélecteur en position haute pensant mettre ainsi en service l'automatisme qu'il commande, mais il s'agit d'un sélecteur à positions multiples et l'automatisme est ainsi mis en veille (modèle de mode d'action des commandes).

Généralement les erreurs du type C ou D sont dues à une utilisation de mauvais modèles de poste de travail, conséquence d'un entraînement insuffisant ou d'un entraînement fait sur un simulateur différant du poste de travail réel.

E/ Le pilote a programmé sur le FMS* une descente depuis 20000 pieds avec une phase de réduction de vitesse de 300 à 250 nœuds en passant à 10000 pieds et un atterrissage automatique sur la piste 05

* Un waypoint est un point arbitraire de navigation, sans réalité physique, défini par le contrôle aérien et déterminé par ses coordonnées géographiques, longitude et latitude, ou par sa position en distance et relèvement par rapport à un point géographique connu (balise ou aéroport par exemple).

Gauche. Mais une modification de la piste d'atterrissage de 05 Gauche à 05 Droite, demandée par le contrôle d'aéroport lorsque l'avion est en descente à 15000 pieds est rapidement reprogrammée par le pilote. Cette reprogrammation a supprimé la phase de réduction de vitesse à 10000 pieds. Le pilote ignore ou a oublié cette caractéristique du FMS qui fait que la reprogrammation d'une phase, ici l'atterrissage, annule la programmation des phases précédentes. Il pense alors que la réduction de vitesse s'effectuera à 10000 pieds et laisse l'avion pénétrer l'espace aérien d'approche au-dessous de 10000 pieds à une vitesse excessive.

Ce type d'erreur est généralement dû à un entraînement insuffisant n'insistant pas assez sur le comportement des automatismes. Il peut être aussi dû à l'utilisation de procédures trop complexes ou a une conception des systèmes imposant un modèle de fonctionnement sophistiqué comportant trop de cas spécifiques.

F/ La chronologie des événements précédents, actions sur les commandes, lectures de paramètres, décisions, transmissions et réceptions de messages a conduit l'opérateur à se bâtir une image "a priori" intérieure ou extérieure.

Par exemple le pilote a placé le sélecteur de train d'atterrissage sur "sorti" et a été perturbé par un message du contrôle aérien. Aussi ne vérifie-t-il pas les lampes de train et pense-t-il que le train est effectivement sorti (puisqu'il a actionné le sélecteur !) alors qu'une panne a fait échouer la manœuvre.

L'opérateur sait qu'une certaine panne s'est produite pendant le quart précédent. Une alarme retentit. L'opérateur, sans vérifier, attribue l'alarme à la panne connue et lance une mauvaise procédure de correction.

L'opérateur agit sur un interrupteur et au même moment retentit une alarme. L'opérateur bâtit une explication que nous qualifierons d'exotique pour expliquer cette coïncidence qui n'est que le fruit du hasard.

Chaque jour l'opérateur doit exécuter la même tâche et en vérifier le bon accomplissement. Chaque jour la vérification se révèle positive. Or, un jour, l'une des manœuvres échoue et le résultat est négatif. Mais l'opérateur ayant toujours observé jusqu'ici un résultat positif ne note pas que le résultat est exceptionnellement négatif et il poursuit la procédure comme s'il était positif.

Chaque jour, sur cet aéroport, le pilote doit virer à droite après décollage. Exceptionnellement le contrôle d'aéroport demande un virage à gauche et en prévient le pilote au moment où il quitte le parking. Bien que le pilote ait accusé réception du message, il oublie la consigne après décollage et vire à droite comme d'habitude.

G/ Au cours de l'approche finale de la piste d'atterrissage, la vitesse est 50 nœuds supérieure à la vitesse recommandée dans le manuel de vol. Mais le pilote ne corrige pas cet écart ne remarquant pas que le risque est élevé de dépasser l'extrémité de piste après l'atterrissage. Il utilise un mauvais modèle de risque.

Il n'est pas évident de reconnaître ce type d'erreur et de faire la distinction avec le cas de type (A) pour lequel le pilote n'a pas noté l'écart de vitesse à cause, par exemple, d'une charge de travail trop élevée avec une atmosphère très turbulente.

L'utilisation d'un mauvais modèle de risque est généralement due à une mauvaise formation et des méthodes d'entraînement n'insistant pas assez sur les différentes conditions à risque.

Lorsqu'une erreur de représentation est identifiée, il est alors nécessaire de définir le type de représentation mentale en cause, Image erronée 1.a, 1.b, mauvais Modèle 2, 3 ou Modèle de Risque 5.

- dans le cas 1.a l'image en cause est l'image de la situation de la machine par rapport à son environnement, position de l'avion par rapport au relief et aux autres avions (on parle alors d'Image 3D), position de la motrice du train sur le réseau et position des autres trains, état de la connexion de la centrale d'énergie dans le système de distribution, .. Ce peut être aussi l'image du réseau de transmission (l'erreur étant souvent la mauvaise identification de l'émetteur et du destinataire d'un message).
- dans le cas 1.b il est nécessaire de préciser de quel système l'opérateur se fait une fausse image, quel était l'état réel du système (marche, arrêt, en panne partielle ou totale,..) et quelle était la représentation que s'en faisait l'opérateur.

---

* Le FMS, Flight Management System est un "super" pilote automatique avec lequel le pilote peut programmer plusieurs phases successives de vol. Le FMS envoie alors des consignes de cap, vitesse, pente et altitude au pilote automatique afin d'exécuter les manœuvres successives ainsi programmées.

- dans le cas 2 il faut définir quel système est en cause et en quoi le modèle de fonctionnement utilisé par l'opérateur était faux (par exemple utilisation d'un modèle trop simplifié non valable dans ce cas particulier de fonctionnement,..).

- dans le cas 3 il faut définir quel mauvais modèle était utilisé (modèle de capture d'information, modèle d'action sur les commandes, modèle d'utilisation des moyens de transmission), quel élément de l'interface et quel type de modèle (localisation, identification, transposition, mode d'action,..) étaient en cause. Cette information est très importante pour préciser si et où il faut modifier la conception de l'interface ou modifier les méthodes d'entraînement et de formation.

Enfin il est utile de préciser si possible l'utilisation d'images ou de modèles retenus "a priori" par l'opérateur, car les remèdes ne reposent pas en général sur des modifications technologiques mais sur des méthodes de formation et d'entraînement mettant en relief ce type de comportement "diabolique" des opérateurs.

Méthodes de Codification et d'Analyse

L'analyse des seuls accidents est insuffisante parce que les accidents sont, heureusement, rares. Il est nécessaire d'analyser les incidents pour y trouver les défauts du système qui sont à l'origine d'accidents potentiels. Mais l'on se trouve face à une tâche de grande ampleur, car les incidents sont très nombreux. Il est ainsi nécessaire de bâtir une méthode de classement des incidents permettant de les grouper par familles afin de les retrouver aisément pour les analyser.

Pour chaque rapport d'incident, nous envisageons deux niveaux d'étude associés à deux différentes méthodes, la Codification et l'Analyse proprement dite..

La Codification

Il faut noter que le niveau Codification a pour seul objet de fournir des moyens et des critères permettant d'extraire d'une base de données des sous ensembles présentant des similarités afin d'identifier des problèmes opérationnels significatifs et de dégager d'éventuels événements précurseurs. Une fois obtenu un sous ensemble de taille raisonnable par tri automatique, il est alors possible d'entamer des Analyses détaillées.

Dans ce but, le processus de Codification doit être relativement simple à appliquer par du personnel connaissant les systèmes en cause (transport aérien, transport maritime ou terrestre, centrale nucléaire, usine de production, etc.) et ne doit exiger qu'un minimum de temps d'exécution.

La méthode de Codification consiste à choisir l'une des rubriques suivantes :

1 - Est-ce que l'un des Facteurs d'Augmentation du Risque (de la liste GARE) est d'une importance telle qu'il constitue l'explication quasi unique de l'incident ? (par exemple, fatigue ou malaise tels que l'opérateur est dans une situation où il ne peut pratiquement pas agir). Un tel cas doit être explicite.[1]

2 - Est-ce que le principal Facteur d'Erreur est une Charge de Travail extrême ?
Ce cas ne doit être retenu que si la Charge de Travail est si élevée que l'opérateur ne peut exécuter sa tâche tout en ayant une conscience parfaite de la situation. Ce cas doit être explicite ou évident implicite.[2]

3 - Est-ce que le principal Facteur d'Erreur est une Chute de Vigilance extrême ?
Ce cas ne doit être retenu que si l'équipage est totalement hors service, aucun pilote dans le cockpit, équipage en train de dormir ou perturbé par un événement extérieur retenant totalement leur attention. Ce cas doit être explicite ou évident implicite. [2]

4 - Est-ce que le principal Facteur d'Erreur est un Lapsus verbal, oral ou gestuel ayant un effet quasi immédiat et évident ? (langue ayant manifestement fourché, maladresse telle qu'un mouvement malheureux de manchette vient couper un moteur). Ce cas doit être explicite ou évident implicite. [2]

5 – Si aucune des rubriques 1 à 4 n'a été retenue, nous sommes en présence d'un cas de Conscience Erronée de la Situation.

Ce cas doit être divisé en trois sous rubriques :

5.1 – Image Externe erronée
La Conscience Erronée de la Situation est relative à la situation extérieure (position de l'avion, météo, état de la piste, autres trafics,etc.)

5.2 – Image Interne erronée
La Conscience Erronée de la Situation est relative à la situation interne au système dont l'opérateur est responsable.

5.3 – Les Images Externes et Interne sont correctes mais l'opérateur utilise un mauvais Modèle de Risque.
.

[1] Explicite signifie que le rapporteur a formellement cité le cas.

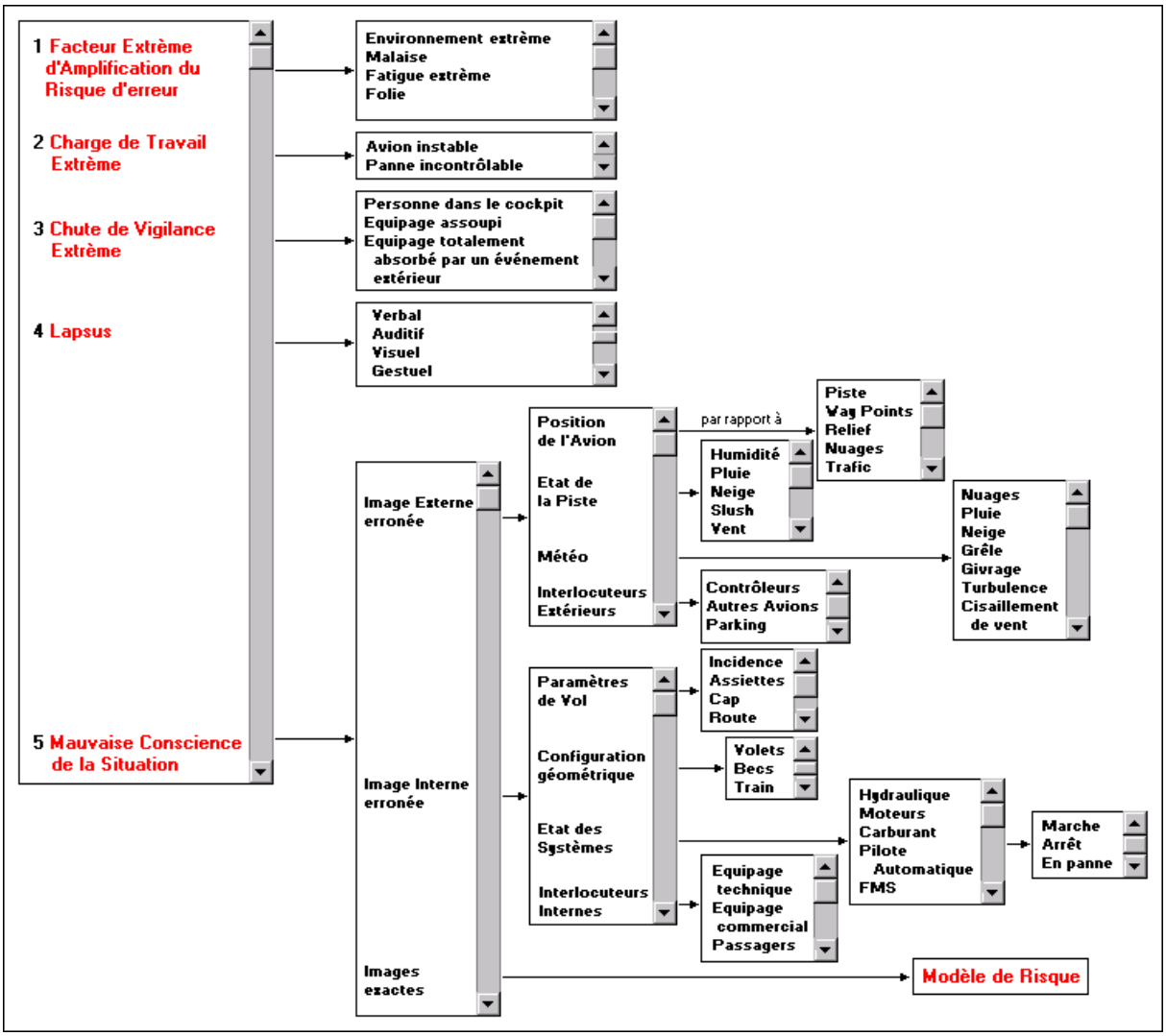
[2] Évident implicite signifie que le rapporteur n'a pas cité formellement le cas, mais que la lecture du rapport ne laisse aucun doute sur sa réalité.

En fonction du degré de détails du rapport, il est généralement possible d'être plus précis et de fournir une sous division des rubriques 5.1 et 5.2. Le plus souvent on pourra définir des listes déroulantes dans lesquelles l'analyste pourra choisir une ou plusieurs rubriques.

En outre l'analyste pourra citer un (ou plusieurs) Facteur d'Augmentation du Risque (s'il ne l'a pas déjà désigné comme cause quasi unique de l'incident).

La planche présentée ci-dessous schématise le processus de Codification.

L'analyste, au niveau de la Codification, doit essayer de préciser, dans le cas d'une Conscience Erronée de la Situation, quelle Image est erronée, Interne ou Externe. Il est aidé par quelques listes déroulantes proposant les divers types possibles d'Images. Les listes présentées ci-dessous ne sont pas exhaustives. Elles ne constituent que des exemples et doivent être complétées par l'expérience.



L'Analyse

A ce niveau l'opération de Codification doit avoir été déjà exécutée, ce que nous supposerons.

L'objectif de l'Analyse est d'obtenir une meilleure compréhension de l'incident en identifiant les Facteurs d'Erreur en cause, s'il en existe d'autres que ceux repérés par la Codification et surtout en mettant en évidence les domaines d'actions possibles pour améliorer la sécurité. Ces domaines sont décrits dans la grille RADOS. La phase d'Analyse est plus détaillée et doit compléter la phase de Codification. Parfois une meilleure compréhension de l'incident peut amener à revoir la Codification. Il faut espérer que cela sera relativement peu fréquent.

L'analyse d'un incident doit se faire de la façon suivante.

- Identifier les conditions générales dans lesquelles s'est déroulé l'incident (utilisation de la grille GARE pour préciser les facteurs d'amplification de gravité). Cette première analyse doit permettre d'estimer la probabilité de retrouver des incidents analogues dans les mêmes conditions générales.

- Identifier l'événement final ayant conduit à la catastrophe ou ayant conduit à une situation potentiellement dangereuse. Ainsi, le franchissement intempestif d'un feu rouge en voiture peut se traduire par un accrochage plus ou moins dramatique (pertes de vies humaines, blessures, dégâts matériels), par un incident plus ou moins fâcheux (prison, retrait du permis de conduire, amende, etc.), par une simple peur rétrospective ou par rien du tout si l'on n'a rien vu !. Quelles que soient les conséquences de l'événement final, il est important d'analyser la succession des événements qui en sont à l'origine.

- Identifier et décrire chronologiquement les événements d'Opérabilité, de Manœuvrabilité, de Sensibilité aux Perturbations ayant conduit à l'événement final.

  En pratique, cette recherche se fait en remontant dans le temps la suite des événements en se posant à chaque étape la question "quels sont les événements préalables qui ont conduit le système et le ou les opérateurs à être dans cette situation ?". La chronologie n'est rétablie qu'une fois identifiés tous les événements et doit être revérifiée en "descendant" le temps.

- Caractériser chaque événement de Manœuvrabilité et de Sensibilité aux Perturbations en utilisant les grilles GAS et GAME.

- Caractériser chaque événement d'Opérabilité en utilisant la grille GAFE. Bien noter que plusieurs événements avec erreurs de l'opérateur peuvent être en cause et ne pas s'en tenir à la dernière erreur.

  L'erreur en elle-même n'a qu'un intérêt anecdotique; mis dans les mêmes conditions un autre opérateur commettra une autre erreur, mais il y a de grandes chances pour qu'il commette une erreur analogue. Ce qui importe de noter, c'est le Type d'Opération au cours de laquelle l'erreur a été commise et le Facteur d'Erreur, c'est-à-dire les conditions dans lesquelles l'erreur a été commise.

  Lorsqu'une "Conscience Erronée de la Situation" est mise en évidence, essayer de l'identifier, de façon aussi complète que possible en fonction de la qualité du narratif et en tenant compte de toutes les autres informations disponibles. Cela devrait confirmer, compléter ou peut-être rectifier le choix fait durant la phase de Codification. "Compléter" devrait être relativement fréquent, parce que la phase Codification n'extrait que les faits les plus saillants, mais d'autres aspects d'une Conscience Erronée de la Situation peuvent apparaître laissant la possibilité d'une identification plus précise. Il sera ainsi nécessaire d'identifier quelles Images sont erronées et si le Modèle de Risque est mis en cause (en se référant aux cinq types de Conscience Erronée de la Situation)

- Compléter, si nécessaire, la liste des Facteurs d'Augmentation du Risque d'Erreur impliqués.

- Une fois la chronologie établie, rechercher pour chaque Facteur d'Erreur ainsi identifié, pour les Facteurs Amplificateurs de Risque et quelquefois pour les événements de Sensibilité aux perturbations et les événements de Manœuvrabilité, le type de Défaut système qui peut être à l'origine de cette situation et le caractériser par une case du Répertoire RADOS.

Il n'y a pas de correspondance systématique entre une case de la GAFE, une rubrique de la GARE, de la GASP ou de la GAME et une case du RADOS, tout au plus des corrélations fortes. Ainsi une erreur due à une charge de travail trop élevée (Cs ou Ca) est en général la conséquence d'une procédure mal adaptée (Ops ou Opa), mais elle peut aussi avoir pour origine une mauvaise conception de l'interface (Hms ou Hma) ou une erreur d'organisation (Oms ou Oma).

- Il se peut par ailleurs que l'on ne puisse identifier sûrement le Facteur d'Erreur et le type de Défaut. Ainsi l'action intempestive sur une commande peut être soit un Lapsus (La) résultant d'une mauvaise conception de l'interface (touches de clavier trop petites et trop rapprochées par exemple) (Hma), soit une erreur de représentation (SPIa) (mauvaise connaissance du modèle de positionnement des commandes) due à un défaut de Formation spécifique (Fsa). L'analyse devra proposer ces différentes possibilités.

- Certains facteurs d'amplification de risque d'erreur identifiés par la grille GARE peuvent avoir pour origine des Défauts Système. Il convient d'identifier ces Défauts au même titre que les défauts à l'origine des événements d'Opérabilité. Ainsi l'inconfort dû au port de casques ou de gants mal adaptés relève de Défauts du type Hm (Interface Homme Machine sur le plan mécanique). La présence de visiteurs intempestifs ou de personnalités, la constitution d'équipages "à risque", relèvent de Défauts d'Organisation.

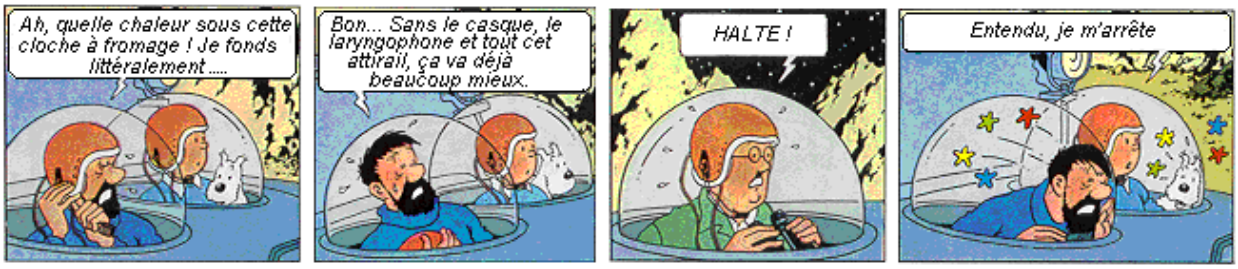
  Bien entendu, les facteurs cités dans la grille GARE n'ont pas tous un Défaut Système pour origine. Ainsi les soucis financiers ou les déboires sentimentaux des opérateurs ne relèvent pas d'un Défaut Système, ce qui ne les empêche pas d'influer sur leur comportement !

  Il n'en reste pas moins que des dispositions spéciales d'organisation peuvent réduire la fréquence d'apparition de ces amplificateurs de risque. C'est ainsi que l'armée de l'air américaine a interdit provisoirement de vol les pilotes dont l'épouse était sur le point d'accoucher !

- Enfin certains événements relevant de la GASP ou de la GAME peuvent avoir pour origine un Défaut système. Par exemple une procédure mal conçue peut conduire à effectuer une manœuvre d'amplitude anormalement élevée, à subir une rafale trop importante (la procédure n'a pas interdit la sortie en mer par vents force 10), à subir une panne dangereuse (procédure de maintenance défectueuse), etc.

- Une fois identifiés les Défauts Système chercher leurs fréquences d'apparition dans les analyses des autres incidents et si nécessaire envisager des mesures correctives.

La fréquence d'apparition d'un Défaut, et du Facteur d'Erreur dont il est la cause, n'est qu'un guide pour décider de l'urgence et de la nécessité d'élaboration d'un remède. La fréquence critique peut se réduire à l'unité si les conséquences potentielles de l'incident sont suffisamment graves et surtout lorsque l'on constate que la catastrophe peut être déclenchée à la suite d'une seule erreur humaine, car la probabilité d'erreur humaine est trop grande pour faire reposer la sécurité sur l'hypothèse que l'opérateur est suffisamment formé et entraîné pour éviter l'erreur.


Ah, quelle chaleur sous cette cloche à fromage ! Je fonds littéralement .....
Bon... Sans le casque, le laryngophone et tout cet attirail, ça va déjà beaucoup mieux.
HALTE !
Entendu, je m'arrête

d'après HERGÉ

La mauvaise climatisation de la cabine est à l'origine de l'incident mais n'en est pas la cause. Ce n'est qu'un facteur amplificateur de risque.

CHAPITRE 12

C'est en forgeant que l'on devient forgeron

Ce n'est pas parce que l'on est un bon opérateur que l'on ne commet pas d'erreur, ce n'est pas parce que l'on a commis une erreur que l'on n'est plus un bon opérateur.

D'après Ellie Wiesel

Les considérations développées jusqu'ici avaient pour but de dégager les principes d'analyse des incidents et accidents rencontrés en service et elles nous ont permis de mettre en évidence un certain nombre de défauts système caractéristiques. Elles vont maintenant nous amener à dresser une liste, non exhaustive, de règles pour aider à la conception des systèmes et à proposer une méthode d'analyse critique d'un système existant avant son utilisation opérationnelle.

Les règles pour la conception d'un poste ne sont pas des règles impératives, mais plutôt des conseils. Il est toutefois recommandé de se poser pour chacune d'elles la question, "La règle a-t-elle été respectée ?" et dans le cas où elle n'a pas été respectée de noter et de justifier les raisons qui l'ont fait abandonner, afin d'améliorer le guide.

LES ERREURS AU MOMENT DE LA CONCEPTION

"L'erreur humaine est à l'origine de tous les accidents. Si les utilisateurs sont mis hors de cause, ce sont les concepteurs qui sont responsables". Voici l'un des lieux communs les plus entendus dans les réunions, symposiums ou congrès traitant de la sécurité.

Il est vrai qu'un certain nombre d'erreurs peuvent être commises par les concepteurs. Quelles sont ces erreurs, comment les réduire, quels sont les outils et les procédures nous permettant de les combattre ?

Lorsque l'on conçoit un nouveau système, c'est avec l'idée, justifiée, de faire mieux que les systèmes en service, "mieux" signifiant des performances supérieures, des coûts de production et d'exploitation inférieurs, une sécurité d'utilisation ou une sûreté de fonctionnement accrues.

La conception nécessite donc le plus souvent une exploration de domaines nouveaux, c'est-à-dire une extrapolation des connaissances. Il est bien évident que toute extrapolation comporte des risques d'erreurs.

Donnons quelques exemples d'extrapolations dans le domaine de la conception des avions.
Sans vouloir être exhaustif, nous pouvons citer

- **A performances égales ou voisines, même domaine de vol (vitesses et altitudes), charge marchande du même ordre de grandeur,**
  - *réduction des masses à vide* (réduction des coûts de fabrication et d'exploitation)

    Utilisation de matériaux nouveaux (composites en particulier), changement d'architecture et de forme, calculs plus "serrés" de pièces élémentaires, méthodes nouvelles d'assemblage ou d'usinage, etc.

    Ces moyens sont valables aussi bien pour la structure de l'avion lui-même que pour les aménagements cabine, les moteurs, les systèmes, les câblages, etc.
  - *amélioration de la finesse aérodynamique*, ce qui réduit la poussée nécessaire des moteurs et donc la consommation kilométrique de carburant.

    Choix d'architecture différente (forme en plan et épaisseur relative de la voilure, taille du fuselage, implantation des gouvernes, etc.). Modification de forme en vol (flèche variable, becs, volets, gouvernes par déformation continue de structure, etc.). Soufflage ou aspiration de la couche limite. Centrage arrière rendant l'avion naturellement instable ce qui augmente la portance (donc la finesse) à même incidence (l'avion est alors rendu artificiellement stable par des systèmes automatiques), etc.
  - *amélioration du rendement des moteurs* conduisant à une réduction de la consommation spécifique (rapport consommation/poussé).

    Amélioration du rendement des compresseurs et turbines par amélioration de leurs caractéristiques aérodynamiques, amélioration du rendement de combustion, optimisation du taux de compression et de la température devant turbine, réalisation d'une architecture permettant de faire varier le taux de dilution en fonction de la vitesse et du Mach, etc.

- *amélioration de la sécurité d'utilisation*

Une augmentation de la sécurité se traduit par une diminution de la probabilité d'accident en utilisation.

Utilisation, par exemple, de systèmes interdisant les dépassements du domaine autorisé pour l'avion ou certains sous-ensembles (interdiction de dépassement de l'incidence de décrochage). Mise en place de systèmes redondants dissemblables limitant les pertes de fonctions vitales.

- *amélioration de la sûreté d'emploi*

Une augmentation de la sûreté se traduit par une meilleure régularité d'utilisation, les systèmes remplissant leurs fonctions avec une probabilité de défaillance diminuée.

Mise en place de systèmes redondants pour limiter les pertes de fonctions interdisant le vol si elles sont détectées avant décollage.

- *augmentation de la durée de vie*

Utilisation de matériaux nouveaux. Changement des méthodes d'assemblage et d'usinage. Systèmes automatiques réduisant la fatigue des structures en évolution ou en turbulence.

- **Changement du domaine de vol (vitesse, distance franchissable) ou de la charge marchande.**

Les moyens sont analogues à ceux que nous venons de citer, mais les extrapolations sont en général plus audacieuses car il ne s'agit pas de "gratter" seulement quelques pour cents.

Le passage de Mach 1 pour les avions expérimentaux au cours des années 50 a été rendu difficile du fait de la mauvaise connaissance, à l'époque, des phénomènes aérodynamiques autour de cette vitesse critique. Les méthodes de calcul, sans ordinateurs, étaient inutilisables et les résultats expérimentaux, inexploitables, parce que les mesures en soufflerie sont perturbées par les multiples réflexions des ondes de choc sur les parois. Seules les expérimentations vraie grandeur, quelque fois douloureuses, ont permis d'accroître les connaissances et de résoudre les multiples problèmes de la barrière sonique.

Passer du vol transsonique au vol à Mach 2 dans la décennie suivante a nécessité un effort également considérable.

On remarquera en outre que les concepteurs de l'époque n'étaient même pas sûrs de l'existence d'une solution pour le programme Concorde. Il s'agissait en effet de concevoir un avion de transport d'une centaine de passagers, d'une durée de vie de l'ordre de trente mille heures, volant à Mach 2 pendant deux heures et demie à chaque étape alors que l'on ne disposait que de l'expérience des avions militaires (durée de vie de l'ordre de cinq mille heures) ne restant en supersonique que quelques dizaines de minutes à chaque vol. Cette remarque prend toute sa valeur lorsque l'on sait que les Américains, à la même époque, ont échoué dans leur tentative de réalisation d'un avion de transport Mach 3 (la technologie disponible à l'époque ne permit pas de trouver une solution. Cet échec a été masqué sous des prétextes écologiques !).

On voit que les possibilités d'erreurs de conception conduisant à de mauvais choix sont multiples. Quels sont les moyens dont disposent alors les concepteurs pour limiter ou corriger leurs erreurs ?

Nous voyons se dégager au premier abord deux types principaux d'erreurs possibles au niveau de la conception :

- les *erreurs matérielles*, du type introduction, recopie ou transmission d'une grandeur erronée, travail sur un plan périmé, erreur de calcul, etc.
- les *erreurs dues à l'utilisation d'un modèle de calcul non valable*.

Les concepteurs disposent de modèles, traduits en code de calcul, permettant de prévoir les performances (masses, résistance structurale statique et dynamique, caractéristiques aérodynamiques, performances globales, etc.).

L'introduction des données de base se fait par des méthodes de CAO (conception assistée par ordinateur) qui limitent les erreurs par leur présentation synthétique sous forme de dessins, de schémas beaucoup plus parlant que des tableaux numériques.

Par exemple le maillage d'une pièce, pour le calcul de résistance à des efforts donnés, se fait de façon quasi automatique, une fois la pièce dessinée; l'opérateur n'intervient que pour des modifications judicieuses en quelques endroits où son expérience lui a montré la nécessité d'un maillage différent ou plus serré. La présentation sur écran du maillage sous forme d'une vue tridimensionnelle tournante lui permet de détecter les anomalies d'un seul coup d'œil.

Le résultat des calculs de la masse, de la position du centre de gravité de la pièce, des inerties, est automatiquement stocké dans un fichier général, provisoire ou définitif après accord des autorités. Une possibilité d'erreur pourrait être, pour prendre un exemple simpliste, l'entrée d'une mauvaise masse volumique du matériau. Aussi est-il nécessaire de l'introduire, non sous forme d'une valeur numérique (on peut se tromper d'un ordre de grandeur en ne positionnant pas correctement la virgule ou se tromper de

chiffre au clavier !), mais en désignant le matériau sur une liste alphabétique préétablie. Bien entendu, le choix du matériau doit être confirmé par présentation du nom en clair du seul matériau choisi et par accord de l'opérateur. On retrouve la règle classique "il ne faut jamais avoir à introduire une nouvelle fois une grandeur dont la valeur est déjà stockée". Il en va de même pour les coordonnées de l'origine et les cosinus directeurs des axes du trièdre de référence dans lequel est calculée la pièce, ainsi que pour les cotes principales figurant sur le plan d'ensemble. Ces dernières grandeurs doivent figurer dans le fichier général sous un nom de code caractérisant la pièce et être appelées par ce seul nom de code en le désignant à l'écran sur la liste des noms de code.

Enfin, quelques programmes de CAO comportent des modules permettant d'automatiser certaines opérations, telles que recopie d'un même circuit, d'une même pièce suivant un schéma préétabli, recherche, à partir d'un schéma de principe, de disposition optimale des pièces répondant à des critères d'encombrement, d'économie, etc. Ces opérations automatiques, non seulement font gagner du temps de conception, mais évite également des erreurs en supprimant les opérations manuelles de passage du schéma théorique, facile à interpréter par le cerveau humain, à la disposition pratique quelquefois moins évidente.

Ceci ne constitue qu'un exemple des règles de conception, élémentaires et bien connues, à suivre pour limiter les erreurs.

Celles-ci peuvent se réduire à quatre règles de base

- disposer d'un fichier unique de données (ce fichier doit être organisé en sous-fichiers pour faciliter la recherche des données),
- ne jamais introduire "manuellement" une grandeur qui existe déjà dans le fichier.
- présenter les résultats sous forme de schémas, graphiques, plans cotés, vues 3D, etc. plus faciles à lire synthétiquement qu'un tableau de chiffres.
- automatiser toutes les opérations répétitives, fastidieuses et mal adaptées au cerveau humain.

Ces règles sont faciles à énoncer. Elles ne sont pas aussi faciles à mettre en pratique et demandent une étude soignée de l'organisation du projet.

Les méthodes de vérification peuvent également être complétées par la fabrication de maquettes d'installation qui jouent un rôle analogue à celui des présentations 3D sur écran. Ces maquettes sont, grâce aux méthodes modernes de présentation 3D, de moins en moins utiles pour vérifier que le dessin ne comporte pas d'incompatibilités spatiales. Par contre, elles peuvent se révéler très utiles pour les études d'accessibilité intervenant dans les études de maintenabilité. Il n'est pas évident par ailleurs d'évaluer les possibilités d'accessibilité, de démontage et de montage de pièces sur une seule présentation 3D. Des programmes spécifiques facilitent cependant ce type d'étude et permettent de se passer des maquettes d'installation.

Les méthodes de CAO disponibles pour certains types de systèmes (en particulier les systèmes électroniques), vont jusqu'à la simulation du fonctionnement du système en réponse à des entrées variées. C'est un excellent moyen pour vérifier que le système que l'on vient de concevoir répond bien au cahier des charges. Par contre, il peut être utile de compléter certaines études par des simulations spécifiques. Par exemple, les modèles de calcul aérodynamiques permettent de prévoir les coefficients aérodynamiques d'un avion, mais il est nécessaire de les introduire dans des modèles de calcul de mécanique du vol pour voir si les performances et les qualités de vol sont satisfaisantes. En effet, quelques règles de l'art permettent de prévoir le bon ou le mauvais comportement d'un avion, connaissant quelques coefficients aérodynamiques importants (ce qui constitue un bon guide préliminaire pour le concepteur), mais ces règles sont en général insuffisantes. Seul un passage au simulateur permet de valider les choix effectués. Rappelons toutefois que ces vérifications ne sont valables que dans la mesure où les modèles utilisés sont valables (attention aux extrapolations dont nous reparlerons plus loin !).

Les systèmes devenant de plus en plus complexes, un certain nombre de méthodes d'analyses est devenu nécessaire pour détecter des fonctionnements néfastes qui peuvent apparaître dans des circonstances particulières et rares, difficilement prévisibles par le simple bon sens, au seul examen des schémas de principe. Ce sont les méthodes du type Sneak Analysis (Méthode de détection des causes insidieuses). Ce genre d'outil est sûrement destiné à être développé comme aide à la conception.

Bien entendu les quatre règles énoncées plus haut ne sont destinées qu'à limiter les erreurs du genre lapsus calami, ce mot s'appliquant, par généralisation audacieuse, à l'erreur matérielle de frappe de la mauvaise touche au clavier, à l'utilisation d'un plan périmé, à l'oubli de recopie d'un circuit ou d'un élément de circuit, à la "faute" de calcul. Elles ne couvrent pas les erreurs de modèles de calcul que nous allons examiner maintenant.

L'ingénieur dispose de toute une panoplie de moyens destinés à vérifier ou infirmer les choix effectués avec les modèles de calcul existants.

Ces moyens vont de l'essai partiel sur éprouvettes, maquettes, éléments échelle un, aux essais sur prototypes.

Les *essais sur éprouvette* sont par exemple utilisés pour déterminer ou confirmer les caractéristiques élémentaires d'un matériau nouveau, d'une nouvelle méthode d'assemblage ou d'usinage.

Les *essais sur maquettes* en soufflerie fournissent les caractéristiques aérodynamiques de l'avion ou de certaines de ses parties. Les conditions de similitudes exactes (nombre de Reynolds et nombre de Mach identiques en vol et en soufflerie) n'étant pas réalisées bien souvent, pour des raisons technologiques de taille de maquette entre autres, ces essais ne fournissent pas directement les coefficients aérodynamiques de l'avion projeté. Ils sont plutôt utilisés pour vérifier la validité des modèles de calcul dans des conditions assez voisines de la réalité et permettre une extrapolation moins hasardeuse.

Des *essais de fonctionnement et de fiabilité de systèmes* sont souvent effectués sur des sous-systèmes prototypes placés dans des conditions d'ambiance aussi réalistes que possibles avec simulation, par calcul des sollicitations d'entrée. Par exemple, les chaînes de commande de vol électro-hydrauliques sont testées avec simulation des ordres d'entrée venant du pilote; les réactions de l'avion (mécanique du vol) sont calculées pour introduire par des vérins les efforts aérodynamiques simulés sur les gouvernes. De même, les ordres du pilote automatique en réponse aux mouvements de l'avion sont introduits comme entrées complémentaires aux ordres du pilote (le pilote automatique peut être le système réel lui-même ou, dans un premier temps, un système simplement simulé lui aussi). Là encore, la simulation n'est pas complète. Même si les modèles de mécanique du vol sont valides, les conditions d'ambiance ne sont pas toujours suffisamment représentatives (pression, température, vibrations, déformation de structure, etc.). Ces essais peuvent donc détecter certaines erreurs de conception mais ne les détecteront pas toutes.

Les *essais de structure* permettent de soumettre des parties de l'avion (demi-voilure, fuselage, train, volets, becs, empennage, gouvernes, etc.) à des sollicitations statiques (efforts mécaniques avec simulation quelques fois d'ambiance thermique) ou dynamiques (essais de fatigue, mécanique ou thermique). Ces essais permettent de valider les calculs de résistance aux efforts que l'on estime devoir survenir au cours de vols réels et de déterminer la marge disponible entre les efforts maximaux estimés en vol et les efforts mesurés conduisant à la rupture. Là encore une incertitude demeure puisque l'on soumet la structure, réelle, à des efforts dont la grandeur et la répartition ne sont que les résultats des calculs et essais aérodynamiques. Une autre incertitude provient du fait que les cellules d'essai sont construites avec des méthodes de fabrication en général différentes des méthodes de fabrication série.

Un autre phénomène limite la résistance des structures, c'est le phénomène de flottement (flutter chez les anglo-saxons). Ce phénomène se traduit par l'excitation d'un mode de vibration sous l'effet de forces aérodynamiques instationnaires dues aux déformations de structure provoquées par un autre mode de vibration. Par exemple, la vibration de flexion en envergure d'une gouverne provoque des variations locales de forces aérodynamiques qui excitent la vibration en torsion de cette gouverne. Ce phénomène peut conduire à des ruptures en fatigue et dans certains cas (flottement explosif) se traduire par des ruptures statiques quasi instantanées. Là encore on dispose de modèles de calcul, combinant le calcul des modes vibratoires des structures et le calcul des forces aérodynamiques instationnaires dues aux modes vibratoires. Les méthodes de calcul des forces aérodynamiques sont sujettes à caution dans le domaine transsonique. Les mesures de modes de vibration sont effectuées au sol et ne donnent que les modes à vitesse aérodynamique nulle (la "rigidité" de la structure en vol, donc ses modes de vibration, dépend des efforts aérodynamiques globaux auxquels elle est soumise). Des essais en soufflerie sur maquette souples "dynamiquement semblables" constituent un autre moyen d'approche du problème. On voit néanmoins que les extrapolations sont tributaires de nombreuses hypothèses sur la validité des modèles que les expériences en laboratoire ne sont pas toujours susceptibles de confirmer.

Restent enfin les essais du ou des prototypes. Ils fournissent sans conteste une bonne estimation des performances et des qualités de vol de l'avion. Ils peuvent ainsi valider les modèles de calcul de mécanique du vol dans le domaine réellement exploré. L'extrapolation aux "domaines interdits en vol" perd de son imprécision et en justifie l'exploration au simulateur. Par des mesures judicieuses de pressions et de températures en quelques points de la structure et quelques mesures, par sonde laser, du champ des vitesses au voisinage des parois, un recoupement des prévisions des caractéristiques aérodynamiques permet de valider les prévisions en la matière, et donc de confirmer les estimations de charge utilisées dans les essais statiques et les essais de fatigue de structure, de valider les modèles de champs aérodynamiques dans les entrées d'air, etc.. Des mesures d'amortissement en vol des modes de vibration de la structure permettent également de recouper les estimations des caractéristiques de flottement.

Un dernier type d'étude reste à effectuer et c'est l'un des points les plus délicats actuels. Il s'agit de vérifier la non nocivité des agressions externes venant de l'atmosphère et ou de la pollution électromagnétique.

L'atmosphère, rafales, cisaillements de vents est désormais relativement bien connue. Il n'en a pas toujours été ainsi. Par exemple, lors de la mise au point de Concorde nous ne disposions que peu d'informations sur les turbulences que l'on pouvait rencontrer aux altitudes de croisières de cet avion, altitudes supérieures à celles des avions de transports subsoniques. La réponse de l'avion aux perturbations atmosphériques est calculable par des méthodes relevant de l'aérodynamique et de la mécanique du vol si l'on connaît les perturbations maximales à couvrir.

Par ailleurs, les avions modernes utilisent des systèmes électroniques qui peuvent se révéler sensibles aux perturbations électromagnétiques, perturbations d'origine naturelle (orages, rayonnement cosmiques), d'origine humaine (installations de production et de transport électrique, installations industrielles) ou d'origine interne (interactions entre systèmes électroniques eux-mêmes, ordinateurs, téléphones portables individuels des passagers). Ces perturbations, surtout les perturbations industrielles, sont encore mal connues et des études sont à faire pour les préciser, mais il est hautement probable que quelques accidents ont eu ces perturbations pour origine.

Un dernier problème se pose enfin aux concepteurs des avions modernes. Les ordres entre le manche et les gouvernes, entre les manettes de gaz et les moteurs circulent maintenant par l'intermédiaire de câblages électriques et d'ordinateurs. Par exemple le pilote envoie, avec le manche, un ordre d'augmentation de pente et c'est l'ordinateur qui envoie les ordres aux gouvernes (par l'intermédiaire des servocommandes) pour obtenir la réponse désirée de façon optimale (précision, rapidité, amortissement, suppression des mouvements parasites, etc.). Il est donc nécessaire de mettre en place des logiciels réalisant ces fonctions de transformation entre la demande du pilote, les réponses de l'avion et l'action sur les gouvernes.

Il est évident que des erreurs peuvent se glisser dans la rédaction des logiciels, au niveau de la rédaction des cahiers des charges et de la rédaction des instructions elles-mêmes. Or une erreur peut avoir des conséquences catastrophiques en provoquant une réponse aberrante de l'avion ou en bloquant le programme rendant l'avion impilotable. La vérification des logiciels ne peut se faire par des méthodes d'essais analogues à celles utilisées pour l'estimation de fiabilité des matériels. Il ne sert à rien de faire "tourner un logiciel" en le sollicitant par des valeurs d'entrée répétitives. Il faudrait trouver une méthode assurant que toutes les combinaisons possibles des valeurs d'entrée ont été examinées et l'on n'est jamais sûr de l'exhaustivité.

Les solutions à ce problème sont diverses.

Une organisation rationnelle des logiciels faisant appel à des langages haut niveau réduit les risques d'erreurs (mais ne les élimine pas tous). Des méthodes de vérification systématique des organigrammes de calcul, des listes de variables, etc. ont été mises au point. Il est hors de propos de les expliciter ici.

Certains ont préconisé la rédaction des logiciels par des équipes indépendantes. Mais des erreurs communes peuvent subsister, dues par exemple à des erreurs de logique dans le cahier des charges ou dues à des méthodes de programmation identiques utilisées par les deux équipes. Nous avons déjà cité le cas d'un sous-programme de calcul des racines carrées, donnant des résultats aberrants dans le cas des carrés parfaits, utilisé par deux équipes indépendantes partageant la même bibliothèque !

Il n'en reste pas moins que l'on est actuellement incapable d'estimer la probabilité de panne d'un logiciel donné, avec des méthodes analogues à celles utilisées pour estimer la probabilité de panne d'un matériel.

La seule solution consiste donc à faire de la redondance, non pas en utilisant plusieurs ordinateurs indépendants fonctionnant avec le même logiciel (seule la défaillance du matériel est couverte par cette solution ce qui n'est toutefois pas inutile), mais en utilisant des ordinateurs dissemblables fonctionnant avec des logiciels dissemblables. Par logiciels dissemblables nous n'entendons pas des logiciels rédigés par des équipes différentes avec des langages différents. Une telle solution couvre les erreurs de programmation mais ne couvre pas les erreurs de logique du cahier des charges. La dissemblance doit s'étendre jusqu'au cahier des charges lui-même. L'idéal est d'utiliser d'une part des ordinateurs digitaux avec un cahier des charges prévoyant toutes les fonctions nécessaires à l'optimisation du vol, d'autre part des calculateurs analogiques (dissemblance du matériel et nécessairement dissemblance du cahier des charges) avec un cahier des charges ne prévoyant que les fonctions minimales nécessaires à la sécurité du vol (Voir chapitre 2).

En conséquence, si le programme des ordinateurs digitaux "se plante", le vol et le retour au terrain sont assurés par les calculateurs analogiques, la mission n'étant plus remplie mais l'avion étant sauvé.

On voit ainsi que l'ingénieur dispose de nombreux moyens (nous ne les avons pas tous cités), pour réduire les incertitudes et éliminer une grande partie des erreurs de conception dues aux imperfections des modèles.

Nous venons de voir ainsi comment limiter les deux types d'erreurs que nous avons cités.

Il existe un troisième type d'erreur de conception que nous n'avons pas encore envisagé dans ce chapitre.

Ces erreurs sont commises chaque fois que le concepteur ne tient pas compte des caractéristiques de l'opérateur humain, futur utilisateur chargé du pilotage ou de l'entretien de la machine.

Nous avons abondamment décrits les défauts d'interface homme machine pour ne pas les répéter ici.

Un grand nombre de règles de conception limitant les erreurs d'interface sera rappelé plus loin.
Elles relèvent toutes du bon sens mais nous avons mis près de quarante ans d'expérience à les rassembler. En définitive, le bon sens, chose au monde la mieux partagée, comme chacun sait, est peut-être tellement partagé qu'il faut y ajouter quelques grains d'hellébore pour perfectionner les recettes de sécurité !

Notons que la mise au point de l'interface nécessite de nombreuses vérifications sur simulateurs puis sur prototype et enfin sur le système réel en début de mise en service, en faisant appel aux avis des futurs utilisateurs. L'expérience montre en effet que toute solution élaborée autour d'un tapis vert ou d'une planche à dessin et jugée géniale par l'ensemble des concepteurs peut se révéler stupide dès que l'on peut en voir une réalisation pratique. Il est indispensable, insistons sur ce point fondamental, d'essayer les solutions sur maquette, sur simulateur, sur prototype en présence des futurs utilisateurs. Le chapitre 13 précise cette notion de simulation.

Cette dernière démarche comporte cependant bien des écueils.
Bien souvent, nous en avons des exemples dans le domaine des transports terrestres, on présente le nouveau poste de travail à quelques opérateurs peu préparés, au cours d'une réunion formelle en présence de responsables de haut niveau. A la question "Que pensez-vous de ce nouveau poste, avez-vous des critiques à formuler ?", la réponse est bien souvent "Non, monsieur le Directeur, ce nouveau poste nous semble parfait". Et tout le monde quitte, satisfait, la réunion; les utilisateurs ont été consultés !
Le problème est quelquefois différent dans d'autres domaines mais pas plus simple.
Bien souvent l'utilisateur moyen est peu ouvert aux innovations. Voilà dix ou vingt ans qu'il travaille sur le même système. Il en connaît tous les défauts et sait en tenir compte. Changer de machine, c'est changer d'habitudes, perdre une qualification durement acquise. Cet état d'esprit se manifeste, au cours de la formation sur un matériel nouveau, par des remarques du style "Mais sur le 737 ce n'était pas comme ça, il y avait quatre opérations à faire et maintenant on obtient le résultat en une seule opération ! C'est complètement déroutant. C'est trop simple, les jeunes ne vont plus savoir piloter, etc. !". Nous avons rencontré cette attitude aussi bien chez les pilotes de ligne (l'allusion au 737 n'est pas innocente) que chez les conducteurs de machines de chantiers de travaux publics.
Il est donc nécessaire de faire appel à des utilisateurs ouverts aux nouveautés, mais quand même capables de critiques. Il faut faire aussi le tri de ces critiques car il y a en général autant d'avis que d'utilisateurs.
Dans le domaine des transports aériens, l'avis des pilotes d'essais, fondamental pour la mise au point, est néanmoins insuffisant car ils connaissent mal la vie de tous les jours des pilotes de ligne, avec leurs servitudes et leurs contraintes.

En un mot, le problème est extrêmement complexe et à chaque incident un peu grave on recueille les doléances de toutes parts. "Ah ! si l'on nous avait écoutés", s'écrient les uns. "Nous avons recueilli tous les avis favorables et tous les avis contraires, comment faire un choix ?", s'écrient les autres.

Bien souvent les utilisateurs regrettent de ne pas avoir été consultés et les concepteurs regrettent de ne pas avoir pu consulter plus d'utilisateurs ou d'en avoir consulté trop ! Chacun ignore que les syndicats d'un côté et les directions des compagnies aériennes de l'autre, ont des politiques prudentes limitant la consultation des utilisateurs. Il faut se trouver des arguments juridiques pour se défendre en cas de pépins graves !

Cette constatation sévère va nous servir d'introduction au chapitre 14, sécurité et problèmes juridiques.

Pour le moment examinons les règles de conception sur le plan de l'ergonomie des interfaces.

REGLES DE CONCEPTION D'UN POSTE

Nous allons retrouver, bien entendu, des règles déjà citées, mais regroupées de façon différente pour servir plus facilement de guide, alors qu'elles n'ont été évoquées jusqu'ici que comme conséquences du comportement de l'opérateur.

Que l'on nous pardonne de nous répéter, mais nous savons qu'il est nécessaire de taper plusieurs fois sur un clou pour l'enfoncer durablement !

a/ Détecter les circonstances où une erreur unique de l'opérateur peut conduire à la catastrophe, afin d'en réduire la fréquence d'apparition.

C'est la même raison qui a conduit à faire en sorte qu'une défaillance unique d'un système ne conduise pas à une catastrophe, car nous ne pouvons démontrer que la panne unique a une probabilité suffisamment basse pour être négligée. La solution pour les systèmes réside dans la redondance dissemblable.

Il nous faut entreprendre une démarche analogue pour l'erreur unique de l'opérateur.

On peut exiger de l'opérateur qu'il fasse de l'auto-vérification de ses actions. Cette démarche, en vogue dans certaines industries car elle limite le nombre d'opérateurs affectés à une tâche, présente un risque important car il est très difficile à chacun de se remettre en cause, comme le montrent tous les exemples d'erreurs de représentation diaboliques. Chacun sait combien il nous est difficile de relire, pour correction, un texte que nous venons de rédiger alors que nous détectons plus facilement les erreurs dans un texte dont nous ne sommes pas l'auteur

Une seconde solution, résultant de cette dernière remarque, consiste à "redonder" l'opérateur en lui adjoignant un ou plusieurs autres opérateurs dont la tâche consiste à vérifier les actions du premier. Cette solution améliore sans doute la sécurité, mais elle se révèle souvent insuffisante car une telle redondance manque de "dissemblance". Les opérateurs ont tendance, dans la même situation et plongés dans la même action, à commettre les mêmes erreurs et à ne pas voir les erreurs des autres (ce n'est pas le cas de la relecture, après coup, du texte d'un autre, c'est, ici, le cas de la vérification, "sur le tas", des actions de l'autre). Nous avons donné de nombreux exemples où deux ou trois opérateurs commettent, en équipe, la même erreur.

Enfin, comme nous l'avons souligné au chapitre 6, une bien meilleure solution consiste à faire effectivement de la redondance dissemblable en adjoignant à l'opérateur un automatisme qui peut avoir différents modes d'action,

- interdire l'action erronée elle-même.

  Entrent dans cette catégorie tous les systèmes de détrompage, par exemple les dispositifs mécaniques interdisant des montages erronés, les dispositifs de verrouillage n'autorisant que des enchaînements prédéterminés de diverses commandes.

  Font partie également de ce type de solution, tous les dispositifs automatiques inhibant les actions de commandes conduisant à des dépassements du domaine autorisé (automatismes sur les avions modernes, interdisant le dépassement d'une incidence limite, de la vitesse maximale ou du nombre de Mach maximal, etc.)

- prévenir l'opérateur qu'il vient de mettre son système dans une situation qui, à terme, peut devenir dangereuse et lui indiquer de façon simple et claire la procédure à suivre pour revenir dans un état sûr.

  Ainsi un système automatique détecte que l'avion est en descente, à basse altitude, basse vitesse, moteurs réduits et train d'atterrissage non sorti. Il prévient le pilote que cette configuration peut être dangereuse à terme si le vol se poursuit ainsi jusqu'à l'atterrissage.

  On ne peut envisager dans un tel cas un système interdisant l'atterrissage en remettant par exemple automatiquement les gaz (il faut bien se poser dans le cas d'une panne de train !) ni sortant automatiquement le train (il se peut qu'exceptionnellement le pilote veuille se poser train rentré, par exemple en cas d'atterrissage de détresse sur une piste très courte).

  Les systèmes, dits de test de cohérence, entrent dans cette catégorie (systèmes vérifiant que la configuration du système est cohérente avec la phase en cours de la mission). Ces systèmes constituent une application de la philosophie de l'approche par état que nous avons décrite comme remède aux erreurs de représentations provoquées chez les opérateurs par leur appréhension chronologique des événements.

- prévenir l'opérateur qu'il s'apprête à faire une manœuvre dont les conséquences peuvent être graves et lui demander de confirmer sa volonté d'action par une seconde manœuvre qui ne doit pas être réflexe.

  Ce sont de telles dispositions que l'on rencontre sur les micro-ordinateurs personnels lorsque l'on s'apprête à détruire un fichier de données ou à formater un disque ou une disquette non vierges.

  Sur ordre de destruction ou de formatage, apparaît un message avertissant des conséquences de cet ordre et demandant confirmation. Cette confirmation doit être faite sous une forme qui ne soit pas réflexe, par exemple taper sur la touche "Entrée" au clavier. Ce doit être une opération demandant à l'opérateur une action cognitive, par exemple taper les trois lettres "OUI" au clavier. Un système automatique ne peut interdire la manœuvre car elle peut, dans certains cas, se révéler utile et sans les conséquences graves dont seul un opérateur humain peut être juge.
- limiter les conséquences de la manœuvre erronée en agissant automatiquement sur le système.

  Par exemple, un dispositif coupe la traction sur une locomotive lorsque le mécanicien déclenche une action de freinage (voir l'accident de la gare de l'Est au chapitre 7).

  Un système automatique interdit, sur véhicule routier, le blocage des roues même si, par réflexe, le conducteur écrase le frein (système type ABS).

  Si le mécanicien d'un train ne respecte pas la signalisation d'arrêt imposé par un carré fermé, un dispositif automatique (le KVB) freine le train pour lui éviter de pénétrer dans une zone à protéger (en particulier pénétrer sur une voie déjà occupée par un autre train).

  Ce dernier exemple est très caractéristique. Répétons ce que nous avons déjà écrit. L'expérience montre en effet que malgré tous les efforts de formation et les mises en garde, les mécaniciens "brûlent" "trop souvent" les carrés et qu'à chaque incident la hiérarchie constate, avec tristesse et étonnement, que ces erreurs sont commises par des opérateurs sérieux, compétents, conscients de leurs responsabilités et bien entraînés.

  Nous avons mis le terme "brûlent" entre guillemets pour bien montrer que cette erreur n'est pas le résultat d'une action délibérée de la part des mécaniciens qui, en réalité, ratent l'information "carré fermé" et l'ignorent involontairement.

  Nous avons dit "trop souvent". Cela ne signifie pas que les mécaniciens font tous les jours ce type d'erreur. Ces erreurs sont heureusement rares, mais encore trop fréquentes pour entrer dans le domaine du risque résiduel admissible.

  Or le fait de passer un carré fermé relève de l'erreur quasi unique. En effet, un signal d'avertissement précède le carré fermé. Mais si ce signal précurseur n'est pas perçu, pour diverses raisons, perturbation extérieure, chute de vigilance due à la fatigue, surcharge de travail momentanée, habitude de voir le signal "toujours ouvert", etc. tout porte à croire que le carré fermé ne sera pas non plus perçu car non prévu. Bien sûr, ce signal précurseur est utile et il diminue la probabilité d'erreur, mais il est insuffisant pour ramener la probabilité d'erreur dans un domaine acceptable. Il est donc nécessaire d'adjoindre au carré un système automatique n'en rendant pas catastrophique le franchissement intempestif.

b/ Fournir des informations réellement utiles et non ambiguës.

Il s'agit de fournir des informations en rapport direct avec la situation réelle du point d'état par rapport aux limites et avec l'état réel du système.

Cette règle peut sembler évidente. Elle est en réalité bien souvent transgressée. Au risque de nous répéter rappelons quelques exemples caractéristiques que nous avons déjà décrits.

L'accident de la centrale nucléaire d'Harrisburg (Three Mile Island) en est l'exemple le plus spectaculaire. Le tableau de contrôle de la centrale comportait un voyant indiquant, non pas la position de la vanne de décharge du circuit primaire de refroidissement du cœur, mais l'ordre de fermeture (ou d'ouverture) envoyé par le système de surveillance de la pression primaire. L'opérateur interpréta la signalisation de vanne comme une signalisation de position fermée. Or, malgré l'ordre de fermeture envoyé par le système automatique de surveillance de pression (c'est cet ordre qui était signalé), la vanne était restée coincée ouverte. Le circuit de refroidissement primaire s'est donc vidé ce qui a conduit à la fusion partielle du cœur.

Une erreur analogue est à l'origine de l'accident du DC 10 des Turkish Airlines à Ermenonville (voir chapitre 7). Le pilote avait eu confirmation de la fermeture correcte des soutes à bagages par la consultation des voyants correspondants sur son tableau de bord. Or la porte d'une des soutes était en réalité incorrectement verrouillée, d'où son ouverture en vol, une dépressurisation brutale, la rupture du plancher cabine et la destruction des câbles de commande de la gouverne de profondeur. La non-signalisation de cet état dangereux provenait du fait que le micro-switch de contrôle indiquait la position de la poignée de fermeture et non la position des verrous.

Un opérateur particulièrement musclé avait réussi à mettre la poignée en position fermée en forçant sur les verrous qui n'étaient pas en bonne position. Là encore l'alarme ne signalait pas le non-verrouillage lui-même de la porte mais la position d'un dispositif qui ne lui était pas strictement lié.

Nous retiendrons qu'une *information doit avoir une signification non ambiguë pour limiter les erreurs de représentation*.

c/ Ne pas fournir des informations difficiles à interpréter.

Il ne faut pas obliger l'opérateur à effectuer des opérations mentales compliquées pour en déduire la marge par rapport aux limites, l'écart par rapport aux consignes ou l'état réel du système.

L'exemple que nous avons déjà cité est celui de la présentation d'un paramètre sous forme digitale et de sa limite sous forme analogique ou la disposition inverse.

On notera, par ailleurs, que la présentation digitale est néfaste pour le pilotage d'un paramètre car il est très difficile d'estimer la grandeur de l'écart par rapport à la consigne, de saisir le signe de cet écart et son sens de variation, alors que toutes ces données sont évidentes en présentation analogique. Il est ainsi beaucoup plus facile et rapide de lire la vitesse sur un tachymètre classique à aiguille que sur un tachymètre numérique. L'opérateur saisit la position de l'aiguille par une opération de reconnaissance de forme et en déduit quasi instantanément si la vitesse est dans un domaine acceptable. Sur un tachymètre numérique, il lui faut interpréter la lecture des chiffres et comparer mentalement le résultat aux limites du moment.

Une règle est de *ne fournir des présentations digitales que pour les paramètres qui doivent être utilisés pour des calculs précis et non pour le pilotage qui doit rester analogique*.

Une fois de plus, insistons sur le fait que les technologies disponibles ont pendant longtemps limité les possibilités de présentation d'information. Il faut comprendre que, maintenant, grâce aux progrès de l'informatique, sur le plan performances et coûts, tout est possible. La seule limitation réside dans l'imagination des concepteurs et dans les habitudes routinières des utilisateurs.

Rappelons la règle "*il faut schématiser et non symboliser*".

d/ Ne fournir que les informations utiles.

Autrement dit, il importe de supprimer toutes les informations inutiles. Cette remarque est évidente mais combien de fois oubliée.

Il est néfaste d'augmenter la charge de travail par la lecture de paramètres inutiles, mais la tentation est grande pour le concepteur d'ajouter sur le tableau de contrôle tel ou tel paramètre sous prétexte qu'il est facilement mesurable et qu'il "peut toujours servir".

Dans certains cas, ajouter des paramètres redondants peut faire naître l'espoir d'obtenir de l'opérateur un contrôle de cohérence. Cet espoir est en général irréaliste, car l'opération de contrôle de cohérence augmente énormément la charge mentale et est très souvent abandonnée par l'opérateur. Elle nécessite en outre des raisonnements complexes et le risque de conclusion erronée est très élevé.

Ainsi dans le cas de la centrale d'Harrisburg (Three Mile Island), l'opérateur disposait de 19 paramètres qui lui auraient permis de conclure à l'ouverture de la vanne de décharge ! Il a interprété de travers quelques paramètres pour justifier l'hypothèse de la vanne fermée et il a complètement ignoré les autres (pourquoi vérifier une hypothèse fermement établie ?). Par exemple la température élevée à la sortie de la vanne a été considérée comme normale car l'opérateur savait que la vanne fuyait quelque peu.

S'il est inutile de présenter des paramètres redondants, il n'est par contre pas inutile de s'en servir pour effectuer un contrôle automatique de la cohérence des informations, et de ne présenter à l'opérateur que le résultat de l'opération de contrôle, sous la forme d'un seul paramètre permettant l'interprétation facile de la situation, la valeur de ce paramètre étant la meilleure estimation possible compte tenu des informations disponibles.

On voit, ici, les techniques de l'intelligence artificielle s'introduire subrepticement ! L'estimation de la meilleure valeur d'un paramètre peut résulter en effet de telles techniques, encore dans leurs premiers

balbutiements. Il n'en est pas moins vrai qu'il est temps d'en prévoir l'utilisation prochaine. Une fois de plus, ces techniques vont poser de faux problèmes de philosophie d'emploi sinon d'éthique.

Nous avons déjà vu proposer l'affichage d'un paramètre global unique, permettant une décision simple et rapide, accompagné de l'affichage de tous les paramètres élémentaires utilisés pour la création du paramètre global. L'intention était de demander à l'opérateur de vérifier la cohérence du résultat proposé par l'ordinateur !

Nous retrouvons ici la démarche naïve déjà prônée dans l'aéronautique à l'occasion de l'introduction, dans le courant des années cinquante, des servocommandes et plus récemment des commandes électriques. Il n'est pas inutile de détailler ces problèmes.

Au début des années cinquante, les avions se sont heurtés au problème de la croissance des efforts aux commandes, liée à l'augmentation de la vitesse aérodynamique. Les pilotes, agissant sur les gouvernes par l'intermédiaire des commandes mécaniques, ne pouvaient plus fournir les efforts nécessaires. Le manche se révélait un bras de levier insuffisant. Il était donc naturel de remplacer la chaîne de commande mécanique par une chaîne comportant un amplificateur artificiel d'effort, la servocommande. Bien entendu, cette amplification nécessitait la mise en place d'une source auxiliaire d'énergie, la pompe hydraulique. Immédiatement se posa le problème de la fiabilité de cette source d'énergie. Il fut donc proposé de mettre en parallèle avec la servocommande, une liaison purement mécanique permettant au pilote de se retrouver en liaison directe avec la gouverne. On voit immédiatement l'aberration d'une telle prescription. Le pilote n'est pas assez musclé pour fournir les efforts, mais on compte sur lui pour les fournir quand même en cas de panne du système destiné à le remplacer!

Les avions modernes ne comportent plus de liaison mécanique entre manche et gouvernes. La sécurité est assurée par une redondance suffisante du système hydraulique.

Au milieu des années 80, on a vu apparaître un nouveau système de commandes, les commandes électriques. Ces systèmes permettent au pilote d'envoyer des ordres de trajectoire à un ordinateur de bord qui commande le déplacement des gouvernes (par l'intermédiaire des servocommandes) afin de respecter les ordres prescrits. Il est alors possible de piloter des avions naturellement instables, l'ordinateur agissant suffisamment rapidement sur les gouvernes pour maintenir l'équilibre même instable.

Cette possibilité de pilotage d'un avion en situation instable ne résulte pas d'un choix vicieux ! On sait depuis longtemps qu'un avion instable, parce que centré arrière, a de meilleures performances qu'un avion stable (la démonstration de cette affirmation sort du cadre de cet exposé), mais cette propriété était inutilisable en pratique puisque l'avion était impilotable. Les commandes électriques permettent enfin de profiter de cette propriété.

Bien entendu une panne d'alimentation électrique ou une panne de l'ordinateur a des conséquences dramatiques puisque la liaison pilote servocommandes ne se fait que par l'intermédiaire de l'ordinateur. On a vu aussitôt de bons esprits recommander de placer en parallèle avec la liaison manche - ordinateur - servocommandes, une liaison directe et mécanique manche - servocommandes pour remédier aux pannes de l'ordinateur ou de la génération électrique. On tombe sur un problème analogue au précédent. On compte sur le pilote pour maîtriser un système instable et remédier ainsi aux défaillances du système qui est seul capable d'assurer l'équilibre !

Dans le cas de la servocommande, on espérait que le pilote pourrait devenir soudainement Goliath en cas de panne hydraulique. Dans le cas des commandes électriques, on espérait voir notre Goliath se transformer de plus en David véloce en cas de panne électrique.

On constate maintenant que la compréhension de certaines situations nécessiterait l'installation à bord d'un système expert destiné à faire l'analyse à la place du pilote. Et bien entendu certains beaux esprits (toujours les mêmes!) proposent de demander au pilote de contrôler le système expert pour en détecter les erreurs de diagnostic! Cette fois notre Goliath - David devrait se doubler d'un Einstein!

La solution ne réside pas dans la surveillance impossible du système expert par l'opérateur mais dans une fiabilité du système telle que la panne en soit jugée raisonnablement improbable. Il nous reste maintenant à mettre sur pieds les méthodes permettant de bâtir des systèmes experts ayant une fiabilité suffisante et des moyens

permettant d'évaluer cette fiabilité. Ceci est une autre histoire, mais la solution ne réside pas dans l'utilisation de l'homme avec ses défaillances et ses faiblesses. Le Goliath - David - Einstein n'existe pas !

e/ Fournir de l'information.

Nous avons déjà insisté longuement sur cette caractéristique de l'opérateur humain qui a besoin de stimuli, en particulier d'informations en provenance de la machine.

Nous renvoyons le lecteur aux chapitres 3, 4 et 5 pour plus de détails sur ce sujet.

Précisons toutefois un point important touchant la reconfiguration d'un système après panne.

Une panne ayant été signalée à l'opérateur par une alarme appropriée, il importe à celui-ci d'effectuer un certain nombre de manœuvre pour retrouver un état sûr, bien que dégradé.

Plusieurs solutions sont possibles pour aider l'opérateur dans cette tâche.

- la solution classique consiste à lui fournir une procédure ou une check-list qui constitue un résumé, de la procédure, un pense-bête permettant de n'oublier aucune opération. Le choix entre procédure détaillée et check-list dépend de la fréquence de la panne. Pour une panne courante une check-list est en général suffisante. Pour une panne rare il est préférable de fournir une procédure complète. Ce choix dépend également de la rapidité d'intervention nécessaire. La difficulté principale réside dans la présentation de la procédure d'identification de la panne et de choix de la procédure de reconfiguration.
- une solution moderne, mise au point sur les Airbus 320,.., 380, consiste, d'une part, à présenter sur un écran le schéma du système en panne avec identification des organes défaillants, d'autre part à afficher sur un autre écran la check-list à appliquer. Sur le panneau de contrôle des systèmes, au plafond, entre les pilotes, la commande du premier organe dont il faut modifier l'état est signalée par l'allumage d'un voyant. L'opérateur exécute alors la première opération indiquée sur la check-list en agissante sur la commande qui lui est signalée par le voyant. Dès que l'état de l'organe est modifié, la première ligne de la check-list s'efface. Par ailleurs le nouvel état de l'organe est signalé sur le schéma (par exemple un robinet d'intercommunication passe sur le schéma de la configuration ouverte à la configuration fermée). L'organe suivant à commander est signalé sur le panneau de contrôle. L'opérateur est ainsi guidé pas à pas dans l'exécution de la procédure. Il se peut que la procédure soit à compléter lors d'une autre phase de vol, par exemple au cours de l'approche précédent l'atterrissage. Dans ce cas l'opérateur est prévenu qu'il aura à compléter la reconfiguration ultérieurement et la check-list complémentaire est affichée en temps voulu. Enfin une fois la procédure terminée, le nouvel état de l'avion est signalé en précisant les changements de performance dus à cet état dégradé (par exemple augmentation de la distance de freinage en cas de perte d'un système hydraulique).

On peut dès lors se poser la question suivante.

A partir du moment où les automatismes sont programmés pour indiquer sur quelle commande l'opérateur doit agir, ne serait-il pas aussi simple de faire agir directement ces automatismes sur la commande sans exiger une manœuvre manuelle de la part de l'opérateur ?

La réponse à cette question est OUI, il faut totalement automatiser, si la reconfiguration doit être faite très rapidement dans des conditions où la sécurité risque d'être compromise par une manœuvre erronée ou trop lente. C'est le cas par exemple de la panne moteur au décollage qui est effectivement entièrement automatisée avec action sur les commandes de vol pour maintenir une trajectoire saine ainsi que sur les commandes moteurs pour obtenir le maximum de poussée disponible sur les moteurs restants et pour couper l'alimentation du moteur défaillant.

Par contre la réponse est NON pour toutes les autres manœuvres n'exigeant pas une habileté exceptionnelle de la part des opérateurs. La reconfiguration manuelle permet aux opérateurs de prendre conscience progressivement du nouvel état des systèmes et donc d'en être parfaitement informé une fois la manœuvre effectuée.

Une tentative de reconfiguration entièrement automatique avait été entreprise par EDF dans le cadre d'une recherche, sur simulateur d'étude, de commande informatisée d'une centrale nouvelle génération. Les opérateurs ont unanimement rejeté la solution proposée. Ils constataient qu'une alarme survenait avec une avalanche de messages signalant toutes défaillances secondaires, notaient que les alarmes disparaissaient progressivement suite aux actions des automatismes jusqu'à ce qu'un dernier message signale que tout était rentré dans l'ordre (nous simplifions un peu !). Ils se plaignaient tous de ne rien comprendre "il s'est passé quelque chose; tout est rentré dans l'ordre, mais c'est très désagréable de ne pas savoir ce qui s'est passé !".

Ainsi la reconfiguration manuelle guidée par l'ordinateur permet de fournir toute l'information utile à l'opérateur sur le nouvel état du système.

f/ Fournir des informations permettant la prévision.

Les informations de ce type sont les informations sur l'état du système à contrôler et sur le sens et l'amplitude de ses variations. Disposant de ces informations, l'opérateur peut alors prévoir l'évolution du système à l'aide de ses divers modèles de représentation.

Il est évident que les opérations mentales de prévision nécessitent une certaine charge de travail de recueil de données, d'interprétation de la situation présente et d'extrapolation dans le temps.

On a quelquefois cherché à réduire cette charge de travail en présentant à l'opérateur, non la situation, mais la position des commandes permettant de corriger les écarts par rapport aux valeurs de consigne. Incontestablement on supprime ainsi toute charge de travail d'interprétation de la situation et de choix des commandes, mais on supprime, par la même occasion toute possibilité de prévision de la part de l'opérateur. Celui-ci est dès lors obligé de capter en permanence les indications d'ordre de position de commandes, car il n'est pas en mesure de prévoir l'évolution temporelle de ces ordres.

On remplace ainsi une charge de travail intelligente d'interprétation et de prévision par une charge de travail stupide de recueil continue d'informations, l'opérateur se trouvant ramené au niveau d'un servomécanisme pur.

C'est là l'occasion de faire la différence, dans les opérations de "contrôle de processus" entre ce que nous appelons les opérations de conduite et les opérations de pilotage.

Nous appellerons pilotage toutes les actions qui, relevant d'une tactique à court terme, permettent de maintenir ou de faire évoluer un paramètre de pilotage ou un paramètre de fonctionnement de la machine, c'est-à-dire maintenir ou faire évoluer une valeur de consigne.

Les opérations de conduite relèvent d'une stratégie à plus long terme permettant de gérer le processus. Elles portent sur le respect des objectifs de la mission. Elles reposent sur des prévisions d'évolution du processus et sont la conséquence d'opérations de comparaison entre prévision et observation. Ce sont elles qui sont à l'origine des valeurs de consigne pour les paramètres de pilotage, les paramètres de fonctionnement des systèmes, les automatismes.

Les opérations de pilotage peuvent être très facilement automatisées parce qu'elles relèvent d'algorithmes de décision très simples, consistant à réduire les écarts entre valeur de consigne et valeur mesurée.

Dans un contrôle de processus, il y a toujours intérêt à soulager l'opérateur des opérations de pilotage en le remplaçant par des automatismes, tout en lui laissant le travail noble de conduite pour lequel les algorithmes de décision sont beaucoup plus délicats à élaborer. En général, il n'est pas facile de prévoir toutes les situations possibles, donc de prévoir toutes les réponses nécessaires.

Par suite il importe de supprimer à l'opérateur toutes les tâches subalternes de pilotage pour lui laisser l'esprit libre pour l'analyse de la situation, l'appréciation de son évolution et le choix des stratégies qui en résultent. Nous avons présenté en détail le problème de l'automatisation au chapitre 6 après avoir examiné les caractéristiques positives de l'opérateur humain.

Il a été quelquefois proposé un pilotage des processus dit "aux alarmes". Autrement dit dans un tel mode de commande, on ne présente aucune valeur des paramètres d'état du système. On ne fait que signaler l'approche d'une limite par la mise en service d'une alarme.

On voit tout de suite combien ce mode de conduite est en contradiction avec la recommandation proposée dans ce paragraphe. On oblige l'opérateur à une veille permanente, sans la moindre possibilité de prévision. Il ne sait ni quand ni quelle alarme va se signaler. La situation est évidemment insupportable.

Enfin, parmi ces recommandations, il ne faut pas oublier la présentation des modes des systèmes automatiques et la présentation des modes qui doivent s'enchaîner normalement. Ainsi au cours d'une montée jusqu'à une altitude sélectée, il est nécessaire de prévenir le pilote que le mode suivant, mise en palier, va être mis en service.

Ainsi, à titre d'exemple, sur avion, l'indicateur de mode (FMA, Flight Mode Anonciator, Indicateur de mode du pilote automatique) doit présenter les informations suivantes lors d'une montée en "Open Climb" (Montée plein gaz à une vitesse sélectée par le pilote 300 kt par exemple),

- jusqu'à 29000 ft "Open Climb 300 kt" (Montée Plein Gaz 300 nœuds) en Vert sur la première ligne de l'écran,

Open Climb 300kt	*en Vert*

- de 29000 ft à 29300 ft "Open Climb 300 kt" toujours en Vert et sur la seconde ligne "Altitude Capture 30000 ft", (capture de l'altitude par mise en palier à 30000 ft) en Magenta clignotant,

Open Climb 300kt	*en Vert*
Altitude Capture 30000 ft	*en Magenta Clignotant*

- de 29300 ft à 29500 ft "Open Climb 300 kt" en Vert clignotant et sur la seconde ligne "Altitude Capture 30000 ft" en Magenta fixe,

Open Climb 300kt	*en Vert Clignotant*
Altitude Capture 30000 ft	*en Magenta*

- de 29500 ft à 29800 ft "Altitude Capture 30000 ft" en Vert sur la première ligne sur la seconde ligne "Altitude Hold 30000 ft", (maintien du palier à l'altitude de 30000 ft) et en Magenta clignotant,

Altitude Capture 30000 ft	*en Vert*
Altitude Hold 30000 ft	*en Magenta Clignotant*

- de 29800 ft à 30000 ft "Altitude Capture 30000" en Vert clignotant et sur la seconde ligne "Altitude Hold 30000 ft" en Magenta fixe,

Altitude Capture 30000 ft	*en Vert Clignotant*
Altitude Hold 30000 ft	*en Magenta*

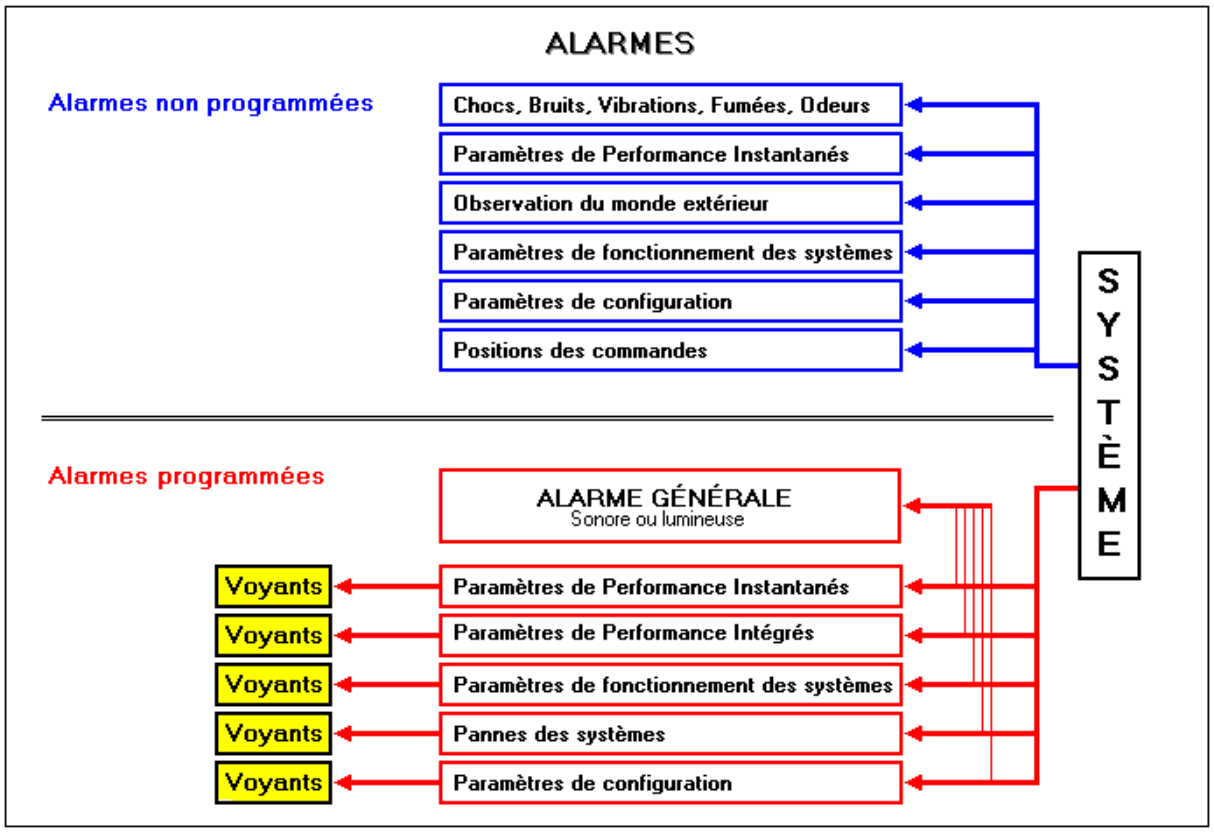
- à 30000 ft "Altitude Hold 30000 ft" en Vert fixe

Altitude Hold 30000 ft	*en Vert*

Les messages en Magenta sur la seconde ligne indiquent le mode futur, le clignotement indique que le changement de mode va avoir lieu. Deux changements de mode sont ainsi signalés, le passage au mode Capture d'altitude à 29500 ft (500 ft au-dessous de l'altitude de palier sélectée) et le passage en tenue d'altitude (à l'altitude 30000 ft sélectée).

g/ Fournir des alarmes qui ne passent pas inaperçues.

Deux grands types d'informations peuvent parvenir à l'opérateur, s'il est en mesure de les recueillir, pour le prévenir d'une anomalie dans la conduite du système. Ce sont les alarmes programmées et les alarmes non programmées dont on trouera les définitions au chapitre 5



Nous avons vu que les alarmes programmées peuvent se classer en quatre catégories :
- les alarmes qui indiquent l'approche d'une limite pour un paramètre de pilotage ou un paramètre de situation
- celles qui indiquent l'approche d'une limite pour un paramètre de fonctionnement d'un système.
- celles qui indiquent un fonctionnement anormal ou la panne d'un système.
- celles qui indiquent que le système n'est pas dans une configuration correcte correspondant à la phase en cours de la mission.

Les alarmes des deux premiers types sont destinées à réduire les probabilités d'événement d'Opérabilité dans la mesure où elles complètent les informations de l'opérateur sur la proximité d'une limite. Nous disons bien "dans la mesure où elles complètent l'information". Comme nous l'avons précisé plus haut, il est aberrant de ne fournir que l'information d'alarme sans affichage permanent de la valeur du paramètre correspondant.

Il est évident que dans la mesure où l'on est capable de détecter l'approche de la limite, il est beaucoup plus judicieux d'en laisser la surveillance et le contrôle à un dispositif automatique, ce qui ne dispense pas de maintenir le système d'alarme en cas de panne des automatismes et reprise du pilotage en manuel.

Les alarmes du troisième type, signalant des pannes de systèmes, sont nécessaires dans la mesure où elles conduisent à une prise de décision ou une action de la part de l'opérateur.

Les alarmes du quatrième type sont beaucoup plus délicates à réaliser car elles nécessitent la reconnaissance automatique de la phase de la mission et de l'état réel du système. Elles sont destinées à éviter les erreurs de représentation, dans le cas où le changement d'état imposé par la mission a été mal effectué ou non effectué par l'opérateur.

Un système permettant la reconnaissance de la phase de vol et la comparaison entre la configuration réelle et la configuration recommandée a été breveté par l'Aérospatiale et la société APSYS, sous le terme général de Test de Cohérence.

Il est évident que la reconnaissance de la phase atterrissage ne peut se faire en repérant la position du train d'atterrissage car cela interdirait de reconnaître une configuration anormale, train rentré, dans cette phase de vol !

Le principe de reconnaissance de la phase repose sur la mesure de paramètres de vol comme l'altitude, la vitesse et le nombre de Mach, quelquefois les régimes moteurs (caractéristiques d'un état si la vitesse est constante), etc. et la constatation que l'ordre d'enchaînement des phases de vol n'est pas arbitraire (par exemple, caricatural, la phase atterrissage ne peut suivre la phase croisière haute altitude). En outre, le système est capable, non seulement de signaler les erreurs de configuration, mais de conseiller sur la configuration optimale compte tenu de contraintes supplémentaires. A titre d'exemple, le système peut reconnaître que la configuration d'atterrissage n'est pas respectée (volets insuffisamment sortis par exemple), mais peut en outre recommander parmi les configurations admissibles, la configuration optimale, par exemple "plein volets" et non "volets en position 3" étant donné la longueur de piste en service et la force du vent. Bien entendu, ces informations doivent être connues du système, ce qui est facile pour la piste en service car le FMGS (Flight Management and Guidance System, système de navigation et de guidage) contient cette information. Il faudra attendre la mise en service des transmissions automatiques des données météo pour obtenir la force et la direction du vent sur la piste. Une étude menée sur le fichier RACHEL (voir Chapitre 8) a montré que si les pilotes avaient disposé d'un tel système, et avaient suivi les instructions proposées, environ la moitié des accidents répertoriés auraient sans doute pu être évités. Dans tous ces accidents, l'erreur initiale était une erreur de représentation se traduisant par une incohérence entre la représentation mentale du pilote et l'état réel du système, et l'accident lui-même ne se produisait que plusieurs minutes après l'erreur initiale. Cela aurait laissé suffisamment de temps au système pour détecter la situation anormale, et au pilote pour la corriger.

La philosophie d'établissement d'un système d'alarme est très délicate à établir. Les quelques règles suivantes peuvent néanmoins servir de guide.

- Limiter le nombre d'alarmes au strict nécessaire car une alarme doit être rapidement perçue et interprétée. Le panneau d'alarmes lumineuses ne doit pas prendre l'aspect d'un "arbre de Noël".

  Une méthode de limitation du nombre d'alarmes du type pannes de systèmes est la hiérarchisation.

  On ne signale que les pannes primaires, c'est-à-dire celles qui sont à l'origine du non-fonctionnement des sous-systèmes qui en dépendent.

  Par exemple, seule la panne d'une génératrice électrique sera signalée, mais non la panne des sous-systèmes qu'elle alimente. La signalisation des pannes secondaires n'est fournie que sur demande de l'opérateur, une fois les opérations de sauvegarde effectuées et lorsque le bilan des systèmes disponibles s'impose.

  On peut espérer simplifier le tableau d'alarmes en remplaçant des alarmes lumineuses par des alarmes sonores. Mais il faut se souvenir qu'une alarme sonore n'est en général pas perçue en cas de charge de travail intense ; elle est plus difficile à identifier (sauf si elle se présente sous forme d'un message vocal) et est plus fugitive.

  En règle générale, il vaut mieux utiliser un signal sonore comme signal général d'alarme, incitant l'opérateur à chercher l'anomalie sur le panneau lumineux et le panneau d'instruments.

- Dans la mesure du possible doubler une alarme du type respect des limites par un système de surveillance et de contrôle automatique de la limite.

  Pour ces alarmes il faut choisir judicieusement le seuil de déclenchement à proximité de la limite.

  Une alarme qui se déclenche trop loin de la limite risque de fonctionner trop souvent et perdre par là son caractère de gravité. Par contre, déclenchée trop tard, elle perd de son efficacité, car elle ne laisse plus à l'opérateur le temps de réagir.

  Si un compromis entre ces deux exigences ne peut être trouvé, c'est que la marge entre le point d'état nominal et la limite est trop étroite. Il faut revoir les consignes d'utilisation et modifier les valeurs nominales.

- Pour les alarmes du type configuration, les présenter si possible sous forme d'une suppression d'une information essentielle, à condition toutefois que cette information puisse être rapidement rétablie par action volontaire de l'opérateur.

  Cette méthode est sans doute préférable à la présentation d'une information supplémentaire, qui risque de ne pas être perçue, parce que non attendue par l'opérateur. N'oublions pas en effet que ce type d'alarme est destiné à combattre les erreurs de représentations "diaboliques" et que l'opérateur n'est pas en situation mentale d'accueil d'une information mettant en doute son modèle.

  C'est ainsi que plutôt que de signaler le train d'atterrissage non sorti en phase d'approche par une alarme lumineuse ou sonore se superposant à une quantité déjà trop grande d'informations, il est peut-être préférable d'occulter l'indicateur de vitesse, instrument que le pilote ne peut ignorer au cours de l'approche et de lui substituer un message d'avertissement du type "Attention, train non sorti".

Dans la mesure du possible, nous l'avons déjà souligné, il est toutefois bien préférable de présenter l'information permettant de saisir l'état du système sous une forme la plus proche possible de la réalité, c'est-à-dire sous une forme analogique, plutôt que sous toute forme symbolique plus difficile à interpréter. Il est probable que la vue directe du train, plutôt que l'interprétation de la couleur de trois lampes, éviterait des atterrissages train rentré par erreur de représentation.

C'est l'occasion de se poser le problème de la présentation du résultat du test de cohérence signalé plus haut. Une simple alarme sonore ou visuelle est sûrement inefficace. L'opérateur est en état d'erreur de représentation diabolique et il risque d'écarter l'alarme sous prétexte que "c'est encore une fausse alarme" ou même ne pas la percevoir. De nombreuses études sont encore à mener pour présenter une alarme "immanquable". Rappelons toutefois que convaincre quelqu'un n'est pas lui imposer le résultat; mais l'amener à faire le raisonnement l'amenant de lui-même à la conclusion. Peut-être faudra-t-il présenter non le résultat brutal du test de cohérence mais les arguments ayant conduit à détecter l'incohérence. Par exemple présenter un message sous la forme "l'avion est à basse altitude, la vitesse est faible, les moteurs sont au régime d'approche avant atterrissage et je constate que le train n'est pas sorti. Si vous devez vous poser, il serait utile de sortir le train ! Qu'en pensez-vous ?".

h/ Limiter le nombre d'actions et faciliter l'élaboration des tactiques et stratégies.

La limitation du nombre d'actions peut s'obtenir, comme nous l'avons vu, en automatisant toutes les actions tactiques simples où l'opérateur n'aurait qu'un rôle de servomécanisme et en lui laissant les opérations de conduite qui en général nécessitent peu d'actions sur les commandes.

L'élaboration des tactiques et des stratégies passe par une compréhension de l'état du système et de son évolution. La compréhension rapide d'un état ne peut se faire en général pour les systèmes un peu complexes, qu'à partir d'une représentation analogique, la représentation digitale étant réservée, nous l'avons déjà dit, à une analyse précise, n'exigeant pas d'action rapide.

Avec l'introduction massive de l'informatique dans les contrôles de processus industriels, on a vu apparaître des présentations d'information sous forme d'états tabulés, sur écran ou, pire, sur imprimante. Ces états permettent a posteriori de suivre de façon très précise l'évolution passée de l'état du système, mais ils ne permettent en aucun cas de suivre son évolution en "temps réel" et d'avoir une évaluation globale et rapide de son évolution passée. L'imprimante, périphérique classique, doit être éloignée de la salle de contrôle, car elle ne peut servir que de "mouchard" et doit être remplacée par des écrans fournissant l'évolution dans le temps des paramètres d'état à contrôler et des limites correspondantes, sous forme analogique et non sous forme digitale. L'opérateur doit disposer également de claviers de commandes lui permettant de faire varier simplement et rapidement la présentation (échelles, paramètres regroupés, fonctions de paramètres, rappel de données passées, présentation dans l'espace de phases, etc.).

Contrairement à ce qui s'est passé dans les industries de production, l'imprimante n'a pas fait son apparition à bord des avions, mais quelquefois la présentation digitale des informations a envahi les écrans, ce qui n'est pas mieux.

Nous avons déjà vu que l'opérateur utilise trois types de modèles pour saisir l'information, les modèles de localisation et de vérification des sources d'information et les modèles d'interprétation de l'information. Il est impératif de simplifier ces modèles par une localisation logique des instruments et une homogénéisation des présentations (échelles, zéros, sens de variation, etc.). On se reportera aux chapitres 4, 5 et 6 pour plus de détails sur ces règles élémentaires de conception des tableaux d'instruments de contrôle.

i/ Étudier la localisation et le mode d'action des commandes.

Nous ne reviendrons pas sur ces points qui ont été largement développés aux chapitres 4 à 6.

Nous rappellerons seulement que la conception des commandes, ou pour être plus précis des actionneurs, relève d'une branche de l'ergonomie que nous appellerons l'ergonomie mécanique et qui traite des formes, tailles, positions, déplacement des commandes compatibles avec les dimensions et les possibilités de déplacement des membres. Cette discipline est très utile et a connu récemment de nombreux développements par la constitution de banques de données ergonométriques, permettant d'introduire des modèles "géométriques et dynamiques" d'opérateurs types dans un système général de conception assistée par ordinateur.

Cette démarche est fondamentale au moment de la conception d'une salle de contrôle ou d'un poste de pilotage. Il est très important de vérifier que les opérateurs pourront voir facilement les instruments sans être amenés à prendre des postures pénibles, qu'ils pourront atteindre, déplacer librement les commandes sans être contraints à des contorsions inutiles et fatigantes. Mais il faut également retenir qu'une telle démarche n'est que le premier pas d'une itération, le deuxième devant faire intervenir les considérations imposées par l'ergonomie

mentale, considérations que nous avons largement développées jusqu'ici. Une commande doit d'abord être facilement manipulable, mais son mode d'action doit être également conforme au modèle mental de l'opérateur.

Le troisième pas de l'itération conduisant à la conception définitive d'une salle de contrôle ou d'un poste de pilotage, passe enfin par des essais grandeurs, de préférence sur des simulateurs d'étude ou sur des machines prototypes, car seule l'expérience réelle avec un opérateur averti du problème peut fournir une critique valable des solutions proposées. On prendra garde toutefois aux opérateurs qui cherchent à mettre leur virtuosité en évidence en élaborant un système de commandes et d'instrumentation qu'ils sont seuls à maîtriser! On se reportera à la fin du chapitre 13 pour plus de détails sur ce type de problème.

j/ Concevoir des schémas sur écrans adaptés aux opérateurs

Quitte à nous répéter voici quelques règles présidant à la conception des schémas sur écran.

- "coller" le plus possible à la réalité, en respectant au mieux les échelles et les dispositions spatiales,
- si le respect rigoureux des échelles est impossible, faire en sorte que l'opérateur ait quand même une idée raisonnable des distances et des proportions en jeu.

  Par exemple, une canalisation et la vanne associée passant un débit de un mètre cube par minute sera représentée plus "grosse" qu'une canalisation et un robinet d'alimentation en eau potable. La liaison avec un système éloigné sera représentée avec une interruption bien identifiable faisant comprendre que l'échelle de distance ne peut être respectée.

  Sur une présentation cartographique respecter les distances (ce point peut sembler évident; or les cartes de navigation en approche aux instruments actuellement utilisées sur les avions de ligne ne respectent pas cette règle, ce qui est manifestement une source d'erreurs).
- éviter les "symboles" pour représenter les organes, en leur préférant des "schémas" simplifiant les détails de construction mais reproduisant l'essentiel de la forme et permettant de saisir d'un coup d'œil la fonction et l'état de l'organe (position ouvert ou fermé, sous tension ou hors tension, etc.).
- éviter de ne représenter les états des organes que par des couleurs conventionnelles. Les différents états seront représentés par des variations de forme du schéma (robinet avec un boisseau bouchant ou non la canalisation par exemple).
- limiter à l'essentiel les renseignements figurant sur le schéma, en particulier les mesures, quitte à les faire apparaître à la demande de l'opérateur ou si un seuil est dépassé (voir le paragraphe concernant les alarmes).
- dans le même esprit les dénominations d'organes seront réduites en nombre à l'indispensable (quitte à pouvoir appeler ces renseignements au moment où ils se révèlent nécessaires).

  On réfléchira à la possibilité de dénominations et en particulier de numérotation différente de celles du concepteur et du constructeur du système. Les risques d'erreurs d'identification peuvent être liés à des numérotations similaires, justifiées pour le concepteur, mais peut-être inutiles ou néfastes pour l'utilisateur. Une dénomination simplifiée est parfois possible ce qui allège d'autant le dessin.
- dans la mesure du possible on s'efforcera à faire tenir le schéma complet sur un seul écran, ce qui peut conduire à un choix de matériel permettant une surface de représentation plus grande.

  Si plusieurs écrans sont nécessaires à la représentation du schéma complet, on prévoira une planche générale permettant de voir le schéma simplifié dans sa totalité et une possibilité de "zoom" faisant apparaître le schéma détaillé.

  Il doit être alors envisagé de disposer de deux écrans, l'un pour le schéma général avec identification facile de la zone zoomée présentée sur le deuxième écran.

  La commande de défilement de la zone zoomée se fera alors par déplacement du repère de zone sur l'écran du schéma général. Ce dernier déplacement se fera par une souris, une boule roulante, un minimanche ou un "touch pad" (voir chapitre 4). Dans la suite de ce paragraphe nous désignerons cette commande par le terme général "souris". Par exemple un déplacement vers la droite et le haut de la "souris" se traduira par un déplacement vers la droite et le haut du repère de zone sur le schéma général (ce qui est intuitif si l'on regarde ce schéma) et par un glissement de l'image sur le deuxième écran représentant le schéma agrandi en sens contraire (ce qui est beaucoup moins intuitif lorsque l'on ne regarde que cet écran).

  Dans le cas d'un seul écran, déconseillé mais quelquefois imposé par la place disponible, le choix de la méthode de déplacement de la zone zoomée, sans repasser par le schéma général, devra être particulièrement étudié, car deux solutions sont possibles; le schéma est considéré comme fixe et la "souris" commande les déplacements de la fenêtre de visualisation sur le schéma (c'est la solution donnée ci-dessus) ou encore la fenêtre est fixe et l'on déplace le schéma sous la fenêtre (ce qui conduit à l'inversion du sens de la commande par rapport à la solution précédente, mais ce qui semble plus facile à interpréter en absence de vision du schéma général).

Il est préférable que la commande de déplacement avec la "souris" ne se fasse pas par désignation d'une direction en "cliquant" après positionnement du curseur sur une bordure (ou un coin de l'écran) ou sur des emplacements sélectionnés sur l'écran (rectangles identifiés Haut, Bas, Gauche, Droite, par exemple). Il est préférable qu'il se fasse en déplaçant la souris dans le sens du mouvement désiré en maintenant le bouton enfoncé (opération de "brossage").

La commande de déplacement ne doit pas être constituée de touches du clavier (touches H, B, D, G ou flèches), car le déplacement doit pouvoir être effectué en gardant les yeux sur l'écran.

D'une façon générale, toutes les manœuvres de commande de la visualisation du schéma (apparition de renseignements complémentaires, appel de données sous forme d'état tabulés ou de courbes, désignation d'organes, etc.), doivent se faire sans passer par un clavier pour éviter la fatigue créée par le passage de la vue de l'écran à la vue d'un clavier. A la rigueur un clavier spécialisé, très simple, constitué de quelques touches seulement, peut être utilisé pour des fonctions très répétitives qu'il peut être commode d'exécuter rapidement sans passer par la "souris" et un menu de désignation.

k/ Lutter contre les erreurs de représentation

La plupart des recommandations faites jusqu'ici ont pour objet de limiter la charge de travail des opérateurs, de maintenir leur vigilance et de limiter les erreurs de représentation des trois premiers types (erreurs sur les images présentes, futures et désirées). Elles sont sans effet pour limiter l'apparition des erreurs des deux derniers types (images "a priori" et modèle de risques erroné)

Une première méthode pour lutter contre les erreurs des deux derniers types consiste

- d'une part à faire connaître aux opérateurs leur existence, existence généralement méconnue; le comportement apparemment aberrant de certains opérateurs au cours d'incidents ou d'accidents connus est souvent mis sur le compte de la négligence et de l'incompétence, mais n'est pas reconnu comme un comportement explicable par la nature même des hommes ("fallait-il être bête ou étourdi pour n'avoir pas vu que la situation était critique !"). L'expérience nous a montré que la mise en évidence de l'erreur diabolique dans l'utilisation du plan manuscrit décrit au chapitre 3 (paragraphe "Les erreurs de modèles ou erreurs de représentation") pour se guider dans un coin de banlieue inconnu, permet à chacun de ne plus se faire "piéger". Cela n'empêche pas l'erreur initiale mais évite de se fourvoyer ultérieurement. Toute discordance entre le monde observé et les indications du plan ne sont pas interprétées comme des erreurs du rédacteur du plan mais comme un signal d'alarme obligeant à faire demi-tour pour retrouver des indications cohérentes !
- d'autre part à montrer aux opérateurs que la mise en erreur diabolique peut se produire, non seulement dans la vie de tous les jours, mais également dans la vie professionnelle et que tout opérateur aussi sérieux, compétent, expérimenté soit il, peut un jour commettre ce type d'erreur.

Dans l'aéronautique, ces deux objectifs peuvent être atteints par des opérations du type connu sous le nom de CRM (Cockpit Ressource Management, formation des équipages à la gestion des informations et des commandes, coordination avec les autres membres de l'équipage). On y insiste sur l'enchaînement des erreurs de représentation, doublées de vol LOFT (Line Oriented Flight Training, entraînement sur des cas de vol réels) au simulateur, vols introduisant des conditions favorisant les erreurs de représentations (les scénarios des vols de l'opération ARCHIMEDE sont des exemples de scénarios à introduire dans ces vols d'entraînement).

Au cours de la deuxième série d'essais ARCHIMEDE, deux membres d'équipage, qui avaient déjà subi une première expérience lors de l'opération précédente (seuls ces deux opérateurs ont été dans ce cas de "redoublement"), ont détecté plus tôt que les autres la chaîne des erreurs en train de se commettre et ont reconnu que l'expérience acquise avait fortement contribué à ce succès. Il est difficile d'en tirer un résultat statistiquement valable; il est toutefois encourageant.

Une seconde méthode repose sur la remarque suivante. L'opérateur ne se remet pas en cause à chaque instant. Le vécu de ses actions ne lui permet pas de douter de leur bien fondé et de leur réussite; "J'ai enclenché le mode Contrôle de Vitesse, donc le mode suivi par le Pilote Automatique ne peut être que celui-ci". Il ne passe pas son temps à revérifier ce qu'il a déjà fait et, pense-t-il, bien fait. Pour le chef de quart de la centrale nucléaire de Three Mile Island, la vanne de décharge était fermée et bien fermée, puisqu'il avait observé cette fermeture sur le panneau d'instruments. Il n'avait aucune raison de remettre en doute ce résultat.

Ainsi est-ce le vécu chronologique des faits, quelquefois mal interprétés, qui interdit pratiquement à l'opérateur de se remettre en cause.

Si par contre un observateur étranger, n'ayant pas vécu le déroulement des faits précédents, analyse la situation, il a des chances de détecter des anomalies car il est obligé pour effectuer son analyse de vérifier la cohérence des informations fournies sans s'en remettre à sa mémoire des faits passés. Ainsi un observateur extérieur analysant le comportement du réacteur nucléaire de TMI, dans l'ignorance des faits passés, aurait sans doute conclu que la vanne de décharge ne pouvait qu'être ouverte, ce que n'imaginait pas, en toute bonne foi, le chef de quart.

Cette démarche est connue sous le nom d'Analyse par État. Elle a été appliquée par EDF dans les centrales nucléaires françaises. En cas d'incident on fait appel à un ingénieur qui n'a pas participé à la conduite, (ISR pour Ingénieur Sécurité Radioprotection) qui fait l'analyse par état et donne un diagnostic indépendant du diagnostic fait par l'équipe de quart. De la confrontation des conclusions peut jaillir l'étincelle réduisant les erreurs de représentation en cours.

Cette méthode n'est pas applicable directement sur toutes les machines, mais il n'est pas impossible de voir à terme un système expert jouer le rôle de l'ISR. Il reste encore bien des progrès à faire dans ce sens et de nombreuses études doivent être menées, ne serait ce que sur la façon de présenter le résultat du diagnostic à l'équipage pour que celui-ci ne le rejette pas en commettant une nouvelle erreur de représentation ("encore une erreur du système expert !"). Nous avons cité plus haut le système connu sous le nom de Test de Cohérence qui doit pouvoir être généralisé à d'autres contrôles de processus.

MÉTHODOLOGIE GÉNÉRALE DE L'ÉTUDE D'UN POSTE
en phase de DÉFINITION

Pour chaque mission ou grande phase ou sous-phase, on établira un schéma opérationnel, c'est à dire un schéma illustrant la suite des décisions/actions requises de l'équipage.

Sont associées à ce schéma :

- Des Règles générales de conception des interfaces (à établir dans le langage et l'organisation du concepteur).
  Les développements précédents décrivant le comportement des opérateurs humains, les défauts systèmes typiques et la réalisation des interfaces serviront de base à l'établissement de ces règles.
- Des Règles propres au projet concerné (telles que Code de couleur, symbologie générale etc.)

Deux démarches sont ensuite conduites, la première descendante, la seconde ascendante.

DÉMARCHE DESCENDANTE

À chaque nœud du schéma opérationnel, c'est à dire à chaque endroit ou une décision ou action est requise de l'équipage, il convient d'examiner:

- Les informations nécessaires pour les prises de décisions (et non les informations complémentaires qui peuvent être utiles par exemple au personnel chargé de la maintenance) et les modes d'accès à ces informations.
- Les actions à faire sur le système pour matérialiser les décisions. Généralement, une action doit être effectuée, action sur une commande, transmission d'information etc.
- Les comptes-rendus de ces actions, c'est à dire les moyens dont dispose l'équipage pour s'assurer que l'action projetée a bien été exécutée..

Pour chacune des opérations précédentes :

- Les passer au crible des méthodes détaillées d'analyse déjà expliquées (accès aux informations, lisibilité, interprétation, informations inutiles... actions élémentaires, accès, commodité, ambiguïté etc.)
- Tester le respect des règles générales. Identifier les difficultés, les éventuels besoins de dérogations ou les demandes de modification de ces règles. Dans ces derniers cas, les justifications appropriées devront être fournies et enregistrées (souci de traçabilité et de vérification de la cohérence des diverses démarches).
- Considérer les erreurs "plausibles" des opérateurs et leurs conséquences. Un certain jugement d'opérationnels expérimentés est utile pour estimer la "plausibilité" ; en effet, il est impraticable de considérer toutes les erreurs physiquement possibles des opérateurs ; dans le doute toutefois, il vaut mieux pécher par excès "d'extension" que par limitation excessive du nombre d'erreurs considérées, l'expérience prouvant que le champ des erreurs rencontrées en service est souvent plus grand que ce que l'on aurait imaginé.
- On considérera notamment les 3 principes suivants :
  1/ Les conséquences ne devront pas être catastrophiques à une échelle de temps compatible avec les conditions opérationnelles.
  2/ Il devra être évident qu'une erreur bien identifiable a été commise.
  3/ La correction devra être facile et le moyen de la faire évident.

Dans cette démarche, si un poste représentatif n'est pas disponible, on pourra s'aider de **maquettes** simples, modestement animées (micro-simulateurs sur PC). Plus précisément, l'usage de tels micro-simulateurs assez tôt dans l'avancement du projet permet de réduire le nombre de corrections à faire ultérieurement lorsque celles-ci deviennent coûteuses ou de réduire le nombre de cas où l'on est obligé de "vivre avec" une solution modestement satisfaisante.

Au cours de cette démarche, il est utile de demander à des opérateurs extérieurs au projet de manipuler les maquettes et micro-simulateurs pour détecter les erreurs plausibles. En effet les concepteurs ne peuvent imaginer les actions "exotiques" possibles qu'ils savent inutiles puisque non programmées. Par exemple ils n'envisageront pas d'utiliser, dans le logiciel en cours de mise au point, la commande CTRL ALT F4 non programmée alors qu'un opérateur extérieur, raisonnant par analogie avec des programmes du commerce, essaiera cette commande pouvant conduire à un plantage catastrophique puisque non prévu.

DÉMARCHE ASCENDANTE

Dans cette démarche, on essaiera de regrouper des sous-ensembles de quelques nœuds consécutifs ou d'une branche entière ou enfin de branches issues d'un même nœud de décision.

A cette phase, on vérifiera des éléments qui n'étaient pas forcément visibles à l'étude de chaque nœud ou que les enchaînements font apparaître, à savoir :

- le respect des règles générales,
- la cohérence des divers éléments entre les travaux élémentaires effectués au niveau de chaque nœud,
- les besoins de dérogation ou de révision des règles générales, toujours avec justification et enregistrement,
- les erreurs non vues précédemment ou dont l'examen sur un plan plus global est utile, avec les mêmes règles d'évaluation que dans la démarche descendante,
- la commodité et l'efficacité des opérations.

Dans ce travail, il sera avantageux s'aider de "**démonstrateurs**" dynamiques (mini-simulateurs !...), permettant de jouer d'une manière assez représentative des éléments ou phases significatives de missions. On notera que ces mini-simulateurs (ou les micro-simulateurs envisagés plus haut) sont des ensembles relativement peu coûteux, assez rapidement développés et d'une grande souplesse d'emploi.

On remontera jusqu'au moment où :

- les questions sont jugées suffisamment dégrossies pour qu'on ne puisse plus sensiblement progresser,
- le "démonstrateur" devient trop complexe ou se révèle incapable du niveau de synthèse nécessaire,
- le passage à un vrai simulateur bien représentatif est possible et jugé nécessaire.

Remarques complémentaires.

- On notera que les questions d'Interface Homme Système (IHS) ne sont pas du **seul** ressort de spécialistes consacrés à l'IHS ; une sensibilisation plus générale des concepteurs est nécessaire (présence dans chaque service au moins de "témoins", ayant suivi une formation rapide).
- Il y a cependant une nécessité de disposer de personnes plus spécialement formées à ces problèmes et plus aptes à les considérer de points de vue opérationnels aussi bien "qu'engineering".

Ceci conduit à constituer de petites équipes intégrées, capables de réaliser **elles-mêmes** les mini ou micro simulations et auxquelles participe de façon fréquente un opérateur.

- Une cellule prospective de recherche appliquée IHS, suffisamment dégagée des contraintes à court terme est utile pour préparer l'avenir.

GUIDE D'EVALUATION D'UN POSTE DE TRAVAIL

L'analyse d'un poste de travail a pour objet l'identification des erreurs potentiellement graves commises par les opérateurs en observant leurs comportements dans l'accomplissement de leurs tâches quotidiennes. L'observation peut aussi porter sur le comportement des opérateurs sur simulateur d'étude et sur simulateur d'entraînement, en prenant garde toutefois aux biais introduits par les techniques de simulation. Il peut être également instructif d'observer les opérateurs en cours de formation. Certaines erreurs, commises en début de formation, disparaissent naturellement au cours de la progression, d'autres persistent et il est très important d'expliquer ces comportements anormaux pour en identifier la cause, mauvaise formation sans doute, mais peut-être Défauts d'interface, d'organisation, etc.

Ainsi l'observation des opérateurs peut-elle permettre de détecter des Facteurs d'Erreur typiques, d'en évaluer les conséquences potentielles, d'estimer leurs probabilités d'apparition et de mettre en place les actions ou les moyens permettant de réduire leurs fréquences (il est utopique de penser que l'on éliminera toutes les erreurs, mais réduire par dix la fréquence d'un Facteur d'Erreur, c'est réduire d'autant la probabilité de l'accident qu'il peut entraîner). Ces méthodes viennent heureusement compléter le Retour d'Expérience exposé au chapitre précédent.

Détecter des Facteurs d'Erreur effectifs ou potentiels nécessite une certaine préparation et la connaissance a priori des types de Facteurs d'Erreurs généralement présents dans les opérations et les Défauts Systèmes qui les favorisent.

Quelques remarques importantes s'imposent avant d'aborder les méthodes d'observation.

Une fois le Défaut identifié, organisation, interface, documentation, formation, réglementation, il paraît évident. On en arrive à se demander pourquoi personne ne l'a découverte plus tôt. Mais il faut reconnaître que détecter les Défauts et les identifier demande un état d'esprit et une méthode qu'il n'est pas évident d'acquérir. Les opérateurs eux-mêmes sont souvent incapables de détecter les erreurs potentielles, et même celles qu'ils commettent réellement. Elles sont en effet pratiquement toujours corrigées, par l'opérateur lui-même ou par un autre membre de l'équipe, et bien souvent elles sont sans conséquences, donc, en toute bonne foi, oubliées une fois commises. Chacun s'habitue aux Défauts d'organisation et de conception, trouve intuitivement des remèdes, des palliatifs qui masquent les difficultés. Chacun modifie les procédures, en les simplifiant quelque fois abusivement. Et ça marche ! Comme les enchaînements d'erreurs critiques sont relativement rares et que ces enchaînements ne conduisent heureusement que peu souvent à la catastrophe, personne ne prend conscience du fait que la situation est potentiellement dangereuse.

Lorsqu'un Défaut d'interface dans un poste de travail est mis en évidence et signalé à un "responsable", la réponse est bien souvent la suivante :

"Oui, bien sûr, ce dispositif n'est pas fameux, mais les opérateurs s'en accommodent très bien. La preuve en est que nous n'avons pas encore eu d'incidents le mettant en cause et voilà dix ans que nous l'utilisons !".

Or rappelons que pour démontrer, par expérience directe, la fiabilité d'un poste (sur le plan de l'erreur humaine entre autres) en tenant compte des objectifs de sécurité que l'on s'impose raisonnablement (moins d'un accident tous les dix millions d'heures) il faut fonctionner plus de 2665 ans sans accident (c'est une règle que les statisticiens démontrent aisément et qui est justifiée dans l'Annexe 2). On voit tout de suite le poids ridicule des dix ans d'expérience sans accident.

Par ailleurs, il faut savoir également que par l'entraînement on peut parvenir à faire faire n'importe quelle tâche à un opérateur. Il suffit d'aller au cirque pour en prendre conscience. Mais il faut ne pas oublier que plus la tâche est difficile, plus le risque est grand de commettre une erreur. La sagesse populaire l'exprime sous la forme imagée "à force de jouer au ###, on finit un jour par gagner !".

Quelque fois la réponse est :

"Modifier ce dispositif ne ferait qu'améliorer le confort des opérateurs. Nous ne pouvons faire des dépenses de confort".

Or le confort est une condition importante de sécurité et non pas un luxe inutile. Toute diminution de la pénibilité d'une tâche augmente les capacités de l'opérateur à faire face aux surcharges de travail et aux événements inattendus. De plus, le terme de confort est utilisé très souvent pour écarter un problème gênant.

Enfin nous avons également entendu:

"Il suffit de demander aux opérateurs de faire particulièrement attention ! Je vais faire une note de service leur rappelant qu'ils se doivent d'être vigilants".

Ces "responsables" oublient que lorsqu'un piège est mis en place, il finit toujours par attraper quelqu'un, et pas seulement les imbéciles, les insouciants et les indisciplinés, quelles que soient les mises en garde qui n'ont d'effet que pendant quelques jours, même chez les plus scrupuleux des opérateurs.

* * * * *

Ces remarques étant faites, regardons quels sont les moyens disponibles pour limiter les erreurs identifiées. L'identification des Défauts Système à l'origine des erreurs est un guide pour l'établissement des remèdes.

Les moyens d'action pour limiter les erreurs sont de six sortes.

⇨ **amélioration de l'organisation**.
- ⇨ en précisant les objectifs des tâches.
- ⇨ en précisant la responsabilité de chacun, ce qu'il doit faire lui-même, ce qu'il ne doit pas faire, ce qu'il peut déléguer, quelles informations il doit transmettre.
- ⇨ en mettant à la disposition des opérateurs les moyens nécessaires en hommes et en matériels.
- ⇨ en présentant les procédures sous forme de consignes claires, faciles à interpréter et à appliquer et non pas sous forme de note de service noyant la procédure au milieu de considérations administratives ou techniques la justifiant. Ce n'est pas une raison pour ne pas justifier les procédures à appliquer, mais c'est un autre problème.

⇨ **amélioration de la conception de la machine et de l'interface homme machine**.
- ⇨ conception de la machine ne conduisant pas à des situations dangereuses.
- ⇨ disposition, forme, lisibilité, dimensions, facilité d'identification, facilité d'interprétation des instruments, etc.
- ⇨ disposition, forme, accessibilité, facilité d'identification, sens d'action des commandes, etc.

Nous sommes déjà revenus longuement sur ces points dans le guide des erreurs de conception car les moyens et les méthodes à mettre en œuvre découlent directement de l'identification de chaque Facteur d'Erreur et de chaque Défaut Opérationnel Système.

⇨ **amélioration de la documentation et de l'information**.
- ⇨ conception de la documentation sous ses aspects matériels, lisibilité (couleurs et graphismes), commodité de manipulation,..
- ⇨ conception de la documentation pour l'adapter aux besoins des opérateurs, intelligibilité des textes et des graphiques, facilité de recherche d'un renseignement,..

⇨ **amélioration de la formation**.
- ⇨ amélioration de la formation de base,..
- ⇨ amélioration de la formation spécifique sur la machine,..
- ⇨ amélioration des méthodes de contrôle des connaissances,..

⇨ **modification de la réglementation.**

⇨ **diffusion de l'information sur les incidents potentiels.**

En attendant que d'autres mesures aient pu être prises, il est fondamental de prévenir les opérateurs de l'existence d'un piège potentiel. C'est insuffisant, on ne peut s'en contenter, mais cela peut provisoirement éviter des erreurs fatales.

Bien entendu, il ne s'agit pas de se contenter de donner des consignes générales de sérieux, de travail, de vigilance, mais de mettre en valeur les pièges identifiés et de décrire quelques moyens, provisoires, pour les détecter et les éviter.

Rappelons quelques règles générales de conception des postes et de rédaction des procédures. Elles vont constituer l'ossature du guide d'observation et de détection des Facteurs d'Erreurs, mais ont été précisées en début de chapitre, en particulier par des exemples, pour être pratiquement utilisables.

⇨ Détecter les circonstances où une erreur unique de l'opérateur peut conduire à la catastrophe, et faire en sorte que ce genre d'erreur ne puisse se produire qu'avec une probabilité suffisamment faible pour être estimée négligeable (système de "détrompage", avertissement du danger de la manœuvre en en demandant confirmation, système automatique interdisant la manœuvre dangereuse, etc.).

Cette règle constitue la règle de conception la plus importante.

- ⇨ Fournir des informations sur les paramètres intéressant la sécurité, et leurs positions relatives par rapport aux limites.
- ⇨ Ne pas fournir trop d'informations (certaines informations sont inutiles parce que redondantes ou sans rapport avec le fonctionnement du système).
- ⇨ Fournir toutes les informations utiles. Cette règle peut sembler évidente et pourtant elle est bien souvent oubliée.
- ⇨ Fournir des informations qui ne soient pas ambiguës.
- ⇨ Fournir des informations faciles à interpréter (les opérations mentales d'interprétation occupent le cerveau de l'opérateur qui peut alors laisser échapper une autre information utile, commettre une erreur d'interprétation ou ne pas avoir le temps d'exécuter les actions nécessaires sur les commandes).
- ⇨ Fournir des informations permettant la prévision.
- ⇨ Fournir des alarmes qui ne passent pas inaperçues.
- ⇨ Concevoir des schémas sur écrans adaptés aux opérateurs.
- ⇨ Ne pas exiger un trop grand nombre d'actions sur les commandes, et faire en sorte que ces actions soient sans ambiguïté, faciles à concevoir et à enchaîner.
- ⇨ Ne pas laisser l'opérateur sans information, son attention est à ce prix.
- ⇨ Laisser à l'opérateur la possibilité de fonctionner "en boucle", c'est-à-dire de corriger ses actions en suivant l'évolution des paramètres d'état à corriger (le fonctionnement en "boucle ouverte" correspond à des actions que l'on qualifie d'actions "exigeant une habileté exceptionnelle de la part de l'opérateur").
- ⇨ Disposer les commandes suivant une logique non contraire à la disposition des organes commandés sur la machine ou sur le terrain.
- ⇨ Faire en sorte que le mode d'action de la commande (pousser, tirer, tourner, lever, etc.) ne soit pas en contradiction avec l'effet de la commande sur la machine.
- ⇨ Lutter contre les erreurs de représentation.

En définitive, l'objectif général de ces règles est essentiellement de réduire la charge de travail de l'opérateur, fonction des quantités d'information qu'il saisit, traite et fournit au système, de maintenir sa vigilance et de limiter les risques de mauvaises interprétations des informations conduisant à des erreurs de représentation de l'état du système, ou à une utilisation de modèles erronés d'actions sur les commandes.

Nous sommes, maintenant, en mesure d'élaborer une **méthode d'observation d'un poste de travail** en fonctionnement réel ou en simulation et de rédiger un guide à l'usage des observateurs. Nous ne justifierons pas les règles énoncées, ces justifications se trouvant dans tout ce que nous avons exposé jusqu'ici. Le lecteur retrouvera par ailleurs de nombreux exemples déjà cités, mais ordonnés suivant une logique différente.

⇨ **Avant de commencer l'observation, essayer de mettre en confiance les opérateurs** (plus facile à écrire qu'à faire sur le terrain, nous en sommes conscients !).

Expliquer

- ⇨ que l'observation, qui va se dérouler sur de nombreuses séances, n'a pas pour objet la détection de fautes et l'application de sanctions; le "Retour d'Expérience" n'est pas le "Retour de Bâton",
- ⇨ que l'observation a pour seul objet la détection des pièges possibles dans lesquels tout opérateur est susceptible de tomber quel que soit son sérieux, son travail et sa compétence,
- ⇨ que tomber dans un piège n'est pas déshonorant,
- ⇨ que si l'on est tombé dans un piège, il y intérêt à le signaler car un autre opérateur ne tardera pas à y tomber lui aussi avec peut être des conséquences plus graves,
- ⇨ que les pièges ont pour origine une conception défectueuse du poste de travail, une organisation ou des procédures mal adaptées, une formation mal assimilée, une documentation défectueuse, une information erronée, et sont indépendants de l'opérateur,
- ⇨ que les Défauts de conception, d'organisation ou de rédaction des procédures, de documentation, d'information ne proviennent pas de l'incompétence des concepteurs et des responsables, (on ne peut tout prévoir) et que seule l'expérience, bien comprise, peut permettre de corriger ces Défauts imprévisibles au départ,
- ⇨ que la détection des pièges est une opération délicate car la plupart des erreurs commises par les opérateurs sont, en général, fugitives, corrigées rapidement et inconsciemment et en général heureusement sans conséquences,
- ⇨ que ce n'est pas parce qu'une erreur détectée n'a pas eu de conséquences qu'il ne faut pas s'en occuper,
- ⇨ que ce n'est pas parce qu'une erreur a déjà été signalée qu'il ne faut pas la signaler à nouveau,
- ⇨ que ce n'est pas parce qu'aucun "pépin" grave ne s'est produit jusqu'ici qu'il n'y en aura jamais,
- ⇨ enfin que le Retour d'Expérience est le seul moyen susceptible d'améliorer la sécurité.

⇨ **Préparer l'observation en se fixant un champ réduit de recherche des erreurs**.

On ne peut observer le comportement de tous les opérateurs en même temps et surveiller l'apparition de tous les types d'erreurs au cours d'une même séance. Il est donc recommandé de se fixer un thème, par exemple le suivi d'une procédure particulière en cherchant à y détecter les conditions favorisant l'apparition d'erreurs liées aux problèmes de charge de travail trop fortes, aux problèmes de pertes de vigilance, aux problèmes de mauvaise représentation ou aux maladresses.

⇨ Charge de travail et perte de vigilance

Il est recommandé de déterminer, au préalable, par observation de l'ensemble du poste de travail les points critiques potentiels (organisation, procédures, sources d'information, moyens de commande, moyens et procédures de transmission) qui risquent de provoquer des erreurs liées à la charge de travail ou les erreurs liées à la chute de vigilance.

Il est recommandé de préparer l'observation en cherchant à déterminer à l'avance les périodes qui risquent d'être critiques en prenant connaissance des tâches à exécuter.

⇨ Erreurs de représentation

Il est recommandé de déterminer, au préalable, par observation de l'ensemble du poste de travail, les points critiques potentiels (organisation ...) qui risquent de provoquer des erreurs de représentation.

Avant chaque séance, on dressera la liste des points critiques qui ont des chances d'être confirmés compte tenu du programme de tâches prévu.

⇨ Maladresses

Là encore, il est recommandé de déterminer, au préalable, par observation de l'ensemble du poste de travail, les points critiques potentiels dus à une mauvaise conception ergonomique du poste (éclairage, taille des commandes, lisibilité des informations, etc.)

Une liste des points critiques à examiner, liste non exhaustive, mais qui pourra être complétée à l'usage, mise à jour et publiée, est fournie en fin de chapitre.

⇨ **Rappelons, et *cette remarque est fondamentale* qu'il n'est pas question de noter les erreurs finales elles-mêmes**, erreurs qui peuvent prendre des formes très différentes et dont les conséquences sont graves ou anodines, mais qui n'ont pas d'intérêt en elles-mêmes. Il ne s'agit pas en effet de combattre ces erreurs-là mais les origines de ces erreurs. Si la charge de travail est trop élevée, l'opérateur peut se tromper en relevant une information erronée, en agissant sur la mauvaise commande, en transmettant une mauvaise information ou en oubliant de la transmettre, en prenant une mauvaise décision, etc. Peut importe cette erreur. Ce qu'il est fondamental de comprendre, ce sont les origines de l'augmentation de charge de travail. Il s'agit donc d'observer les événements qui ont conduit à ces erreurs, et identifier les Défauts de conception, d'organisation, de documentation, de formation, de réglementation qui en ont facilité l'apparition. C'est en effet sur ces événements que nous pourrons agir, en en réduisant la fréquence d'apparition, avec les moyens décrits plus haut.

⇨ Enfin il est impératif, au cours d'une observation de **noter l'état physique** (fatigue, maladie) et **l'état psychosociologique** (soucis personnels, familiaux, professionnels) des opérateurs ainsi que l'environnement de travail (températures extrêmes, présence de personnalités dans le poste, agitation sociale, etc.). Ceci permet de relativiser le degré de gravité des anomalies observées.

La grille GARE, Grille des Facteurs Amplificateurs de Risque d'Erreur, donnée au chapitre 11 peut être utile pour ne pas oublier de noter l'un de ces facteurs.

LISTE DES DEFAUTS SYSTEME TYPIQUES

Cette liste ne constitue qu'un catalogue pouvant servir de pense-bête pour détecter les erreurs potentielles lors de l'étude préalable d'un poste de travail ou pour identifier les causes des erreurs commises lors d'une observation. Elle s'inspire des défauts donnés en exemple au Chapitre 11.

Si un Facteur d'Erreur, potentiel ou observé, est détecté, il est indispensable d'en préciser la nature et son contexte. A titre d'exemple on ne peut se contenter de citer "erreur de représentation due à un mauvais étiquetage d'un voyant d'alarme"; encore faut-il préciser de quel voyant il s'agit, quelle est sa fonction et en quoi étiquetage est-il défectueux (absent de conception, absent par détérioration, illisible par usure, illisible parce que masqué par une coulure de peinture, une tache de graisse, message prêtant à confusion (I et 1, O et 0, B et 8 etc.), symbole difficile à interpréter, etc.).

Une fois de plus rappelons qu'il n'est pas question de décrire l'erreur commise mais les conditions ayant conduit à l'erreur et d'en déduire le Défaut du système à l'origine de ces conditions.

⇨ ORGANISATION

⇨ problèmes de responsabilité d'exécution des tâches

- ⇨ Les opérateurs ne connaissent pas clairement quelles sont les tâches dont ils sont responsables (par exemple répartition des responsabilités entre l'agent de circulation et l'aiguilleur, entre le commandant de bord et le copilote).
- ⇨ Les opérateurs ne connaissent pas clairement le rôle de leur chef, de leurs collègues, de leurs subordonnés.
- ⇨ Les opérateurs ne connaissent pas clairement les objectifs des tâches dont ils sont responsables.
- ⇨ L'organisation a mis en place des opérateurs n'ayant pas la qualification requise (sous qualification et sur qualification).
- ⇨ Les opérateurs s'inventent des objectifs fantaisistes.
- ⇨ Les opérateurs ignorent à quels destinataires ils doivent transmettre des informations.
- ⇨ Les opérateurs se fixent des contraintes a priori s'ajoutant ou se substituant aux contraintes réelles (en particulier ils privilégient la régularité au détriment de la sécurité, avec le souci de "faire l'heure". Les pilotes de ligne tentent l'atterrissage dans des conditions limites plutôt que de remettre les gaz.)
- ⇨ Les règles établies au niveau de l'établissement sont en contradiction avec les règles locales (problème de la décentralisation des responsabilités en matière de sécurité).

⇨ problèmes de moyens

- ⇨ Les opérateurs ne sont pas en nombre suffisant pour exécuter toutes les tâches.
- ⇨ Les moyens matériels mis à la disposition des opérateurs ne sont pas adaptés aux tâches, en nombre et/ou en nature.
  - moyens de mesure
  - moyens de manutention
  - outillage
  - documents aidant la décision (procédures, schémas, abaques, organigrammes de choix de procédure ou organigrammes de décision, etc.)
  - moyens de transmission (émetteur-récepteur portable, téléphone portable, etc.)
  - etc.

⇨ problèmes de méconnaissance des méthodes d'exécution de la tâche (procédures)

- ⇨ Les opérateurs se font un faux devoir d'appliquer les procédures de mémoire sans consulter les procédures écrites.
- ⇨ Les opérateurs ne disposent pas de procédures écrites faciles à consulter et doivent se reposer sur leurs souvenirs de formation.
- ⇨ Les opérateurs disposent de procédures matériellement erronées, pour l'une ou plusieurs des raisons suivantes
  - erreurs de frappe
  - erreur de recopie mécanique (la photocopieuse a "mangé" la dernière ligne d'une page) (d'où la règle élémentaire suivante: une procédure doit être matériellement inscrite dans un cadre; si le cadre n'apparaît pas dans son intégralité, sur la reproduction, la copie doit être rejetée.)
  - erreur de recopie manuelle,

- pages interverties
- etc.

⇨ Les opérateurs n'appliquent pas la procédure recommandée mais une procédure modifiée par l'usage (petit carnet personnel).

⇨ Les opérateurs appliquent la procédure sans en comprendre les raisons et l'interprètent à tort.

⇨ Les opérateurs appliquent les règles d'échange d'information (en particulier rédaction des documents réglementaires) de façon routinière sans en comprendre la justification (par exemple, dépêche d'ouverture de gare expédiée en retard avec un horaire d'envoi antidaté).

⇨ **problèmes de conception de procédure**

⇨ Les opérateurs disposent de documentations sous une forme non adaptée au travail de tous les jours, règlements généraux en particulier.

⇨ Les opérateurs disposent de procédures mal adaptées à leurs besoins (Check List sommaire pour des opérations ponctuelles effectuées rarement, procédures très détaillées pour les opérations de routine).

⇨ Les opérateurs disposent de procédures non mises à jour.

⇨ Les méthodes de mise à jour des procédures sont inexistantes, peu claires ou trop lourdes.

⇨ Les opérateurs disposent de procédures incomplètes ne couvrant pas tous les cas possibles.

⇨ La méthode permettant de déterminer la procédure à appliquer repose sur des critères confus.

⇨ Les opérateurs ne savent pas déterminer si telle procédure les concerne ou non, "dans ce cas là".

⇨ La procédure a été conçue sans se soucier des difficultés d'application,

- l'opérateur doit effectuer seul plusieurs opérations simultanées, nécessitant plus de deux mains,
- la procédure impose des pointes de charge de travail que ne peut assurer le personnel réellement mis en place,
- la procédure ne tient pas compte de la disposition réelle des sources d'information et des commandes sur le poste de travail (action sur une commande en surveillant le résultat sur un afficheur situé à l'autre bout du poste, par exemple)
- la procédure impose une réaction immédiate et rapide à des événements rares alors que l'opérateur n'a rien d'autre à faire que d'attendre (problème de vigilance)
- la procédure ne précise pas les moyens, les outils et les informations à utiliser.
- la procédure ne tient pas compte des erreurs possibles des opérateurs (confusion de commandes ou d'instruments de mesure, voisins, semblables et mal identifiés)

⇨ La procédure comporte des opérations de vérification, mais oublie de préciser les actions à entreprendre en cas de vérification négative. (une méthode de détection de ce type d'erreur consiste à tracer l'organigramme des actions de l'opérateur. On constate qu'un seul embranchement est prévu à la suite de la vérification et que l'organigramme comporte "une patte en l'air").

⇨ La procédure comporte des points de vérification tardifs imposant de repartir à zéro en cas d'échec de la vérification.

⇨ La procédure ne comporte pas de points de rendez-vous pour vérification de l'accomplissement des tâches de chacun des opérateurs avant d'entamer les phases suivantes.

⇨ La procédure, trop générale dans un souci louable de simplification et d'homogénéisation, impose des contraintes inutiles dans un certain nombre de cas. Il en résulte un non-respect de quelques unes de ces contraintes, "justifié" dans certains cas mais anormalement généralisé à tous les cas.

⇨ La procédure est écrite de façon peu claire (par exemple négation sur une interdiction, tel que, "il n'est pas interdit, dans le cas du paragraphe b, alinéa 2 du manuel d'exploitation général de ne pas fermer le robinet si le remplissage du réservoir n'est pas terminé".).

⇨ La procédure ne prévoit pas les actions à entreprendre en cas de panne ou d'indisponibilité temporaire de moyens (par exemple, indisponibilité de téléphone ou fermeture temporaire d'un poste).

⇨ La procédure n'est plus adaptée à une installation qui vient d'être modifiée.

⇨ La consigne locale entre en conflit avec les règlements applicables.

⇨ La procédure ne tient pas compte de l'état d'automatisation du poste (réduction du personnel conduisant à des pointes de charge de travail, longs moments d'inactivité préjudiciable au maintien de la vigilance)

⇨ La procédure ne tient pas compte du fait que l'automatisation a fait perdre certains savoir faire.

⇨ Les consignes temporaires parviennent en retard.

⇨ La durée de validité des consignes temporaires n'est pas précisée.

⇨ Les procédures ne prévoient pas les règles d'échange d'information.

⇨ La procédure prévoit une vérification de bonne exécution par l'opérateur lui-même ou par un second opérateur qui n'a pour tâche, ingrate et fastidieuse, que d'observer que les opérations prévues ont été exécutées et correctement exécutées. Il est bien préférable de faire exécuter de temps en temps, par l'opérateur ou par un autre opérateur, des mesures dont le résultat permet d'affirmer ou d'infirmer la bonne exécution des dernières opérations.

⇨ CONCEPTION DES INTERFACES

⇨ Méconnaissance des règles d'ergonomie mécanique

⇨ L'éclairage est défectueux

- trop fort interdisant la vision de l'extérieur ou la vision des écrans cathodiques,
- trop faible conduisant à des erreurs de lectures (lecture d'un paramètre, d'une étiquette d'identification d'un instrument ou d'une commande),
- changeant la vision des couleurs par rapport à la vision en lumière naturelle,
- provoquant des reflets interdisant la vision de l'extérieur, des écrans cathodiques, des instruments,
- le soleil "masque" l'information, etc..

⇨ Le confort est insuffisant (chauffage, sièges, espace repos, circulations autour des postes, etc.) causant une fatigue inutile des opérateurs ou des risques de maladresses.

⇨ Il n'est pas prévu d'emplacement commode pour placer la documentation en cours d'utilisation, la nourriture ou les boissons.

⇨ Les commandes, les instruments ont une forme, une taille, une disposition spatiale, non adaptées à la morphologie des opérateurs

- touches trop petites alors que, par exemple, l'opérateur travaille normalement avec des gants,
- instruments trop petits, éloignés de l'opérateur en position normale de travail,
- efforts à exercer sur les commandes incompatibles avec la force moyenne d'un opérateur,
- commandes ou instruments hors de portée mécanique ou visuelle de l'opérateur à poste, l'obligeant à des déplacements inutiles et fatigants, etc.

⇨ Les commandes sont disposées trop serrées sur le pupitre ce qui conduit à des risques de d'accrochage intempestif.

⇨ Les commandes critiques ne sont pas protégées par des caches.

⇨ Les afficheurs sont peu lisibles, ce qui induit une erreur de captation de l'information brute

- aiguille grise se déplaçant sur un fond gris face à des graduations grises ou difficilement lisibles,
- afficheur numérique composé de caractères peu lisibles (trop fins, mal dessinés, trop petits, peu lumineux, manquant de contraste avec le fond, etc.),
- échelle mal dessinée (toutes les graduations sont identiques en taille) et valeurs numériques mal positionnées, absentes ou peu lisibles.
- les aiguilles sont placées loin du fond de l'instrument, ce qui induit des erreurs de parallaxe,
- etc.

⇨ Les codes de couleur prêtent à confusion (par exemple, utilisation du mauve, du violet et du magenta avec des significations différentes sur écran cathodique alors que les commandes de luminosité et de contraste, à la disposition de l'opérateur, peuvent modifier les couleurs)

⇨ Étiquetage

- La logique d'étiquetage est celle du concepteur et ne répond pas aux besoins de l'utilisateur

  Les étiquetages des voies ferrées, des aiguilles et des carrés ont été faits de façon indépendante, ce qui conduit à des incohérences à l'utilisation, le même numéro étant, par exemple, utilisé pour une voie, un carré et une aiguille qui n'ont aucun rapport logique entre eux.

  Les étiquetages des robinets, des canalisations, des réservoirs ont été faits, indépendamment, par les concepteurs de ces trois systèmes ce qui les rend incohérents.

- Les étiquettes sont constituées de messages prêtant à confusion.
  - codes trop longs, deux codes d'étiquettes voisines ne différant que par un caractère en milieu de code,
  - utilisation de caractères ambigus,
  - codes de longueurs variables ce qui ne permet pas de vérifier l'intégrité de l'étiquette.
- L'étiquetage d'origine a été remplacé par un étiquetage sauvage, bricolé, compréhensible seulement pour les vieux opérateurs, mais perturbant pour les nouveaux.
- Les étiquettes sont écrites avec des caractères trop petits et difficilement lisibles
- Les étiquettes ont disparu ou sont illisibles parce que salies, usées, partiellement masquées par de la poussière, de la graisse, des coulées de peinture, etc.

⇨ Le système de transmission de l'information est dégradé, par exemple par panne ou insuffisance mécanique, électrique ou électronique, par brouillage ou bruitage (ambiance sonore élevée) ou par mauvaise visibilité (éclairage non nominal, brouillard,...).

A titre d'exemple la manipulation, délicate, d'un étage de fusée exige des transmissions par émetteurs portatifs entre les divers opérateurs. Un haut parleur dans l'atelier diffuse en permanence des

messages de routine du type "on demande à monsieur Dunabla de rappeler le 3615". Les opérateurs, consultés, déclarent qu'ils se forcent à ne pas écouter ces messages qui les perturbent et de toute façon ne les concernent pas!

⇨ **Localisation des sources d'information**

⇨ Les afficheurs sont disposés suivant une logique ne correspondant pas aux besoins des opérateurs, (leur disposition ne tient pas compte de la représentation mentale des opérateurs). Il faut noter qu'il y a toujours une logique de conception des tableaux de bord mais que cette logique n'est pas toujours la bonne, surtout sur les systèmes anciens pour lesquels les problèmes d'ergonomie étaient totalement ignorés.

- les afficheurs ont été disposés sur un pupitre par un concepteur n'ayant aucun souci d'ergonomie (il a suivi le cahier des charges dressant la liste des paramètres à afficher classés suivant un ordre alphabétique, ou les a disposés avec un souci d'esthétique inapproprié, etc.)
- les afficheurs sont disposés de façon à minimiser l'encombrement, ce qui conduit à regrouper arbitrairement des afficheurs dont les fonctions sont très différentes,
- un TCO (Tableau de Contrôle Optique représentant les voies ferrées et leur état d'occupation) est orienté suivant la règle "Paris à gauche", valable pour les plans papiers, mais conduisant à le disposer en sens inverse par rapport aux voies telles que vues du poste

⇨ Les afficheurs sont disposés de façons différentes sur les différents postes de travail qu'un même opérateur est susceptible d'utiliser, ce qui lui demande un effort d'adaptation, à chaque utilisation, favorable aux erreurs de localisation des sources d'information.

⇨ Les afficheurs sont disposés en ne tenant pas compte de la disposition des commandes dont ils dépendent logiquement (le paramètre servant de contrôle à l'action d'une commande est affiché loin de cette commande, les instruments donnant le retour d'information de deux commandes placées côte à côte, sont présentés côte à côte mais intervertis, la commande de gauche étant contrôlée par l'indicateur de droite, etc.)

⇨ **Identification des sources d'information**

⇨ Les afficheurs ont tous la même forme, la même couleur sans étiquetage.

⇨ L'identification du paramètre affiché est faite par des sigles, des symboles difficiles à interpréter.

⇨ La logique d'étiquetage est déficiente (voir les problèmes généraux d'étiquetage en début de guide)

⇨ **Transposition de l'information**

La transposition de l'information brute fournie par l'afficheur en une grandeur utilisable par l'opérateur se fait avec erreur:

⇨ L'échelle est à l'inverse du sens habituel (croissante vers le bas pour une échelle verticale, croissante de droite à gauche pour une échelle horizontale ou croissante en sens inverse du sens d'horloge).

⇨ Le sens de variation du paramètre affiché doit être conforme au sens d'évolution physique de ce paramètre (la vitesse verticale doit être représentée par un déplacement haut bas et non gauche droite).

⇨ L'échelle n'est pas linéaire ce qui rend difficile les interpolations.

⇨ Plusieurs échelles sont disponibles, le choix de l'échelle dépendant d'une commande annexe, ce qui nécessite avant lecture de vérifier la position de la commande de changement d'échelle.

⇨ Plusieurs paramètres sont affichés sur le même instrument avec plusieurs aiguilles ou plusieurs index se déplaçant sur une même échelle, l'identification des aiguilles ou des index se faisant par leur couleur, un symbole, un caractère alphanumérique.

⇨ Plusieurs afficheurs de paramètres de même nature n'ont pas les mêmes échelles (l'opérateur peut transposer un paramètre en utilisant les règles de transposition du paramètre voisin)

- les zéros sont différents,
- les valeurs maximales sont différentes,
- la taille des graduations, leur nombre sont différents.

⇨ L'affichage se fait par voyant de couleur, par clignotement à fréquence variable, d'une façon générale sous une forme symbolique demandant un effort de transposition reposant sur la mémoire.

⇨ L'information est fournie par un signal sonore (une alarme en général) qu'il faut identifier par sa fréquence sonore ou sa fréquence de répétition.

⇨ L'information est fournie sous une forme analogique et il faut l'interpréter par un écart par rapport à une valeur mémorisée sous forme numérique.

⇨ L'information est fournie sous une forme numérique et il faut l'interpréter sous forme de vitesse de variation ou d'écart par rapport à une valeur mémorisée.

⇨ L'information est fournie sur une échelle graduée en pour cents et les consignes sont fournies sous forme de valeurs absolues imposant la transformation des valeurs lues en valeurs absolues.

⇨ Un cas particulièrement pervers est celui de la signalisation en relation non biunivoque avec le phénomène à signaler. Ainsi, on ne transmet pas la position réelle d'un organe à l'aide d'un capteur approprié mais un paramètre plus ou moins en relation avec cette position (par exemple, ordre d'un système automatique de changement de position; en général l'ordre est suivi d'effet sauf s'il y a panne de l'actionneur, alors indécelable par l'opérateur). C'est ce type d'erreur d'interface qui est à l'origine de la catastrophe nucléaire américaine de Harrisburg (TMI) ou de l'accident du DC10 d'Ermenonville.

⇨ Localisation des commandes

⇨ Les commandes sont disposées suivant une logique ne correspondant pas aux besoins des opérateurs, (leur disposition ne tient pas compte de la représentation mentale des opérateurs). Il faut noter qu'il y a toujours une logique de conception des tableaux de bord mais que cette logique n'est pas toujours la bonne, surtout sur les systèmes anciens pour lesquels les problèmes d'ergonomie étaient totalement ignorés).

- les commandes ont été disposées sur un pupitre par un concepteur n'ayant aucun souci d'ergonomie (il a suivi le cahier des charges dressant la liste des commandes classées suivant un ordre alphabétique, ou les a disposés avec un certain souci d'esthétique industrielle, etc.)
- les commandes sont disposées de façon à minimiser l'encombrement, ce qui conduit à regrouper arbitrairement des commandes dont les fonctions sont très différentes (commande agissant sur un paramètre vital à manipuler avec précaution située à côté d'une commande utilisée pour de banales opérations de routine par exemple).
- un exemple anecdotique déjà cité est fourni par la disposition des commandes de mise hors service de quelques escaliers roulants de la RATP (stations Gare du Nord et Halles entre autres). L'étiquette affichée sous l'interrupteur placé à gauche mentionnait "Arrêt de l'escalier droit".

⇨ Les commandes sont disposées de façons différentes sur les différents postes de travail qu'un même opérateur est susceptible d'utiliser, ce qui lui demande un effort d'adaptation à chaque utilisation favorable aux erreurs de localisation des commandes (les claviers d'ordinateurs ont des touches de fonctions réparties de façons différentes, par exemple).

⇨ Les commandes sont disposées en ne tenant pas compte de la disposition des afficheurs des paramètres sur lesquels elles agissent.

⇨ Les commandes sont disposées sur le pupitre en ne tenant pas compte des positions des organes commandés sur le terrain ou sur le tableau de retour d'information d'état des organes commandés (par exemple l'aiguille A est représentée sur le TCO au-dessus de l'aiguille B et la commande de l'aiguille A est placée au-dessous de la commande de l'aiguille B sur le pupitre de commandes).

⇨ Identification des commandes

⇨ Les commandes ont toutes la même forme, la même couleur sans étiquetage.

⇨ L'identification de la commande est faite par des sigles, des symboles difficiles à interpréter.

⇨ La logique de l'étiquetage est déficiente (voir les problèmes généraux d'étiquetage en début de guide)

⇨ Les étiquettes ont disparu ou sont illisibles parce que salies, usées, etc. (rappel des problèmes d'ergonomie mécanique).

⇨ Mode d'action des commandes

⇨ Une commande particulière a un mode d'action différent des commandes du même type ou un mode d'action contraire à l'usage habituel. Par exemple, un robinet particulier s'ouvre dans le sens à visser, un potentiomètre réduit le volume dans le sens à visser.

⇨ La position "Marche" des interrupteurs est arbitraire et varie d'un interrupteur à l'autre, en haut, en bas, à gauche, à droite.

⇨ Les inverseurs sont orientés dans le sens haut-bas (en position haute, l'étiquette du haut est masquée ce qui peut faire croire que c'est la fonction indiquée sur l'étiquette du bas, démasquée, qui est mise en service).

⇨ Le sens d'action de la commande n'est pas homogène avec le résultat de l'action sur l'organe commandé (un déplacement de la commande d'une grue vers l'avant provoque le déplacement à gauche ou vers le bas de la charge commandée).

⇨ L'information de retour de position de la commande présente un défaut correspondant à l'un des critères exposés pour la capture des informations.

Un exemple typique de ces erreurs de conception des commandes est celui des engins de chantier où les commandes à la disposition de l'opérateur se présentent sous forme de leviers parallèles, identiques, à déplacement avant - arrière. L'identification d'un levier ne se fait que par sa position dans la rangée et le mode d'action sur la charge à manipuler n'a rien à voir avec le déplacement de la commande !

⇨ **Transmission des informations**

⇨ Le système de transmission de l'information est dégradé pour des raisons analogues à celles développées pour la captation des informations ou l'action sur les commandes.

⇨ Les opérateurs ne respectent pas les règles d'identification des Émetteurs et des Destinataires lors des transmissions par radio.

⇨ Les opérateurs ne collationnent pas les messages.

⇨ Les numéros ou les fréquences d'appel des postes de sécurités ont des valeurs difficiles à mémoriser et/ou à afficher.

⇨ DOCUMENTATION

⇨ **Défauts matériels**.

⇨ Les opérateurs disposent de documents non mis à jour.

⇨ Les méthodes de mise à jour des documents sont inexistantes, peu claires ou trop lourdes.

⇨ La documentation sur les sources d'information ou sur les commandes est inexistante, incomplète, mal reproduite, difficilement maniable sur le terrain (plans de grandes dimensions ou manuels multiples inutilisables en extérieur) ou encore contient des erreurs matérielles (fautes de frappe sur des codes d'identification d'instruments par exemple).

⇨ La documentation sur les modèles de fonctionnement permettant les décisions est inexistante, incomplète, mal reproduite, difficilement maniable sur le terrain (organigrammes de grandes dimensions ou manuels multiples inutilisables en extérieur) ou encore contient des erreurs matérielles (fautes de frappe sur des codes d'identification d'organes par exemple).

⇨ La documentation sur les moyens et les procédures de transmission est inexistante, incomplète, mal reproduite, difficilement maniable sur le terrain (listes multiples de destinataires ou de fréquences inutilisables en extérieur, caractères trop petits difficilement lisibles sous faible éclairage) ou encore contient des erreurs matérielles (oubli de mise à jour, fautes de frappe sur les codes, les noms de destinataires ou les fréquences par exemple).

⇨ **Défauts de conception.**

⇨ La documentation sur les sources d'information est difficilement compréhensible ou trop dispersée et conduit à des erreurs de saisie de données. Par exemple, il n'est pas clairement précisé que les étendues de mesure des instruments, donnant les valeurs de plusieurs paramètres analogues, ne sont pas identiques (zéros et échelles différentes).

⇨ La documentation sur les commandes est difficilement compréhensible ou trop dispersée et conduit à des erreurs d'action. Par exemple, il n'est pas clairement précisé le sens d'action particulier d'une commande et ses effets parasites sur le contrôle du système.

⇨ La documentation sur les modèles de fonctionnement permettant les décisions est difficilement compréhensible ou trop dispersée et conduit à des erreurs de décision. Par exemple, les organigrammes de décision comportent des ambiguïtés, ou encore ne présentent que le modèle de fonctionnement général du système et renvoient les cas particuliers à des annexes sans en signaler l'importance sur le plan sécurité. Les organigrammes de décision font appel à des conditions quelques fois négatives au milieu de conditions généralement positives.

⇨ La documentation sur les moyens et les procédures de transmission est difficilement compréhensible ou trop dispersée et conduit à des erreurs. Les annuaires ou les listes de fréquences comportent des ambiguïtés ou rendent difficile la recherche d'un code de correspondant. En particulier, les numéros d'appel des postes de sécurité sont noyés dans la liste générale.

⇨ Les schémas fournis sont des schémas de conception et non des schémas d'utilisation, les commandes, les organes, les points de mesure ne sont pas disposés sur le schéma comme sur le poste de travail. La numérotation des organes est une numérotation faite par les concepteurs et inadaptée aux besoins des utilisateurs.

⇨ Les opérateurs utilisent une documentation "sauvage" (carnet personnel dont le contenu est incontrôlable)

⇨ **Information générale**

⇨ Une modification des sources d'information n'est pas signalée ou signalée avec erreurs aux opérateurs (panne de capteur, changement de type d'instrument avec, par exemple, changement d'échelle, déplacement des instruments sur le tableau de bord avec, par exemple, interversion de deux instruments mesurant des paramètres de même nature, etc.).

⇨ Une modification des règles et consignes de conduite, de l'organisation (répartition des tâches par exemple) n'est pas transmise ou est transmise avec erreurs aux opérateurs. Par exemple, le changement de fréquence d'une balise, la mise hors service d'une installation ne sont pas transmises ou sont transmises avec retard.

⇨ Une modification des commandes (position, forme, identification, sens d'action, etc.) n'est pas signalée ou signalée avec des erreurs aux opérateurs (panne, changement de type de commande avec par exemple changement de sens d'action, déplacement des commandes sur le tableau de bord avec par exemple interversion de deux commandes agissant de façon analogue sur le système, etc.).

⇨ Une modification des règles et consignes de transmission, une modification de l'organisation (changement des destinataires des messages), une modification d'un annuaire, n'est pas transmise ou transmise avec erreurs aux opérateurs.

⇨ Les consignes provisoires sont transmises avec retard.

⇨ Les consignes provisoires sont transmises sans préciser les conditions de validité temporelles et locales.

⇨ FORMATION

⇨ **Formation de base**

⇨ Les opérateurs ne disposent pas des connaissances élémentaires suffisantes et adaptées (lecture, écriture, calcul mental ou arithmétique, etc.).

⇨ Les opérateurs ne connaissent pas suffisamment la langue parlée ou ne savent pas lire la langue écrite (en particulier, problèmes posés par l'utilisation de personnels intérimaires étrangers).

⇨ Les opérateurs ne disposent pas des connaissances techniques suffisantes et adaptées (mécanique, résistance des structures, électricité, électronique, informatique, hydraulique, aérodynamique, etc.).

⇨ Les opérateurs ne disposent pas des connaissances suffisantes et adaptées sur les techniques de base (usinage, soudage, câblage, etc.).

⇨ Les opérateurs ne disposent pas des connaissances suffisantes et adaptées sur l'organisation de l'entreprise.

⇨ Les opérateurs ne connaissent pas, ou connaissent mal, les règles générales de transmission de l'information.

⇨ Les opérateurs ne connaissent pas, ou connaissent mal, les règles générales de sécurité et les règles générales de discipline.

⇨ Les opérateurs ne connaissent pas ou connaissent mal les comportements de l'opérateur humain sources d'erreurs ou de défaillances (ils n'ont pas lu Vive les Pépins !).

⇨ **Formation spécifique**

⇨ Les opérateurs ne disposent pas des connaissances techniques suffisantes et adaptées sur les modèles de fonctionnement du système dont ils ont la charge.

⇨ Les modèles de fonctionnement proposés sont trop simplifiés pour couvrir tous les cas de fonctionnement possibles.

⇨ Les modèles de fonctionnement retenus par les opérateurs en formation sont trop simplifiés pour couvrir tous les cas de fonctionnement possibles.

⇨ La formation n'a pas suffisamment insisté sur les particularités des systèmes de présentation d'information et des systèmes de commandes, ce qui induit des erreurs sur les trois modèles utilisés pour la saisie des informations et les quatre modèles utilisés pour les actions sur les commandes.

⇨ Les objectifs des procédures n'ont pas été clairement exposés; en particulier les événements redoutés couverts par les procédures n'ont pas été suffisamment détaillés en précisant les risques encourus en cas de non - application ou d'application partielle des procédures.

⇨ Les documents fournis au cours de la formation sont insuffisamment renseignés, partiellement erronés ou inexistants (voir tous les problèmes généraux de documentation).

⇨ La formation est périmée, en ce sens qu'elle porte sur des systèmes ou des procédures qui ne sont plus en service.

⇨ La formation continue, permettant d'approfondir ou de mettre à jour les connaissances, est inexistante ou insuffisante.

⇨ Les opérateurs ne connaissent pas ou connaissent mal les règles de sécurité spécifiques au système dont ils ont la charge.

⇨ **Simulation**

⇨ Les commandes et les instruments sont disposés de façons différentes sur le poste de travail et sur le simulateur d'entraînement, ce qui demande à l'opérateur un effort d'adaptation favorable aux erreurs de localisation des commandes ou aux erreurs de localisation des sources d'information.

⇨ Les commandes ont une forme et un mode d'action différents sur le poste de travail et le simulateur d'entraînement ce qui demande à l'opérateur un effort d'adaptation favorable aux erreurs d'identification des commandes et de mode d'action des commandes.

⇨ Les instruments sont différents sur le poste de travail et le simulateur d'entraînement ce qui demande à l'opérateur un effort d'adaptation favorable aux erreurs de transposition de l'information.

⇨ Le modèle de fonctionnement du simulateur est trop simplifié par rapport au modèle de fonctionnement réel du système ce qui favorise l'utilisation de modèles de fonctionnement inadaptés aux situations réelles.

⇨ **Contrôle des connaissances.**

⇨ Le contrôle de connaissance se réduit à une vérification des connaissances livresques des opérateurs du type résolution mathématique de problèmes théoriques.

⇨ Le contrôle de connaissance est effectué par des méthodes du type QCM (Question à Choix Multiples).

Cette méthode est très appréciée des services de formation en ce sens qu'elle simplifie énormément la correction des épreuves jusqu'à l'automatiser, mais elle a le défaut rédhibitoire de ne pas estimer correctement les connaissances réelles des opérateurs. Ou bien la réponse de la question relève du simple bon sens et non des connaissances réelles de l'opérateur ou bien la question est posée de façon ambiguë et seule la connaissance a priori du piège permet de répondre correctement (ce qui incite les opérateurs à apprendre par cœur les réponses !).

Il est maintenant possible d'automatiser la correction du contrôle en profitant des méthodes de simulation sur micro-ordinateur obligeant les opérateurs à utiliser leurs connaissances réelles pour résoudre les problèmes pratiques posés.

⇨ Information de Retour d'Expérience

⇨ Les incidents relevés en service n'ont pas fait l'objet d'une diffusion suffisante auprès des opérateurs avec mise en garde pour couvrir, temporairement, des cas analogues (problème de diffusion du Retour d'Expérience entravée par le souci, légitime, d'anonymat).

⇨ Les incidents observés en service par les opérateurs et la hiérarchie de proximité n'ont pas fait l'objet d'un rapport suffisant aux autorités de sûreté

- rapport ne relatant que les conséquences matérielles et non la description des événements à l'origine de l'incident,
- rapport non transmis par crainte de sanctions ou de critiques,
- rapport non transmis car portant sur des événements déjà cités de nombreuses fois, etc.;

Les mauvaises raisons pour bloquer la remontée de l'information sont légions.

⇨ RÉGLEMENTATION

⇨ Les règles imposées n'ont pas un objectif de sécurité mais des objectifs très différents, par exemple assurer la régularité des opérations financières et comptables.

⇨ Une règle, judicieuse à une époque devient caduque ou même néfaste à une autre époque, compte tenu des évolutions de la technique ou des méthodes d'exploitation.

⇨ Deux règles, rédigées par des organismes différents et destinées à traiter des événements redoutés différents face à des types d'agression différents peuvent se révéler contradictoires au moment de leur application.

⇨ La méthode d'élaboration des règles est défectueuse.

Il est très commode d'énoncer une règle de sécurité en imposant un moyen et c'est cette méthode qui est utilisée dans de nombreux règlements. Elle a l'avantage de faciliter la rédaction et la vérification de la règle. Le moyen est décrit en termes techniques et il suffit d'en vérifier la présence et la conformité sur le système réalisé. Nous renvoyons le lecteur au Chapitre 10 pour plus de détails sur le sujet.

d'après GOSCINNY et UDERZO

Une mauvaise interprétation peut être la source d'une erreur de représentation mais conduit toujours à une représentation critiquée.

CHAPITRE 13

Simulateur n.m. Personne qui simule un trouble, un symptôme, une maladie.
Exemple Le simulateur du pavillon 3 vient de mourir.

QUELQUES RÉFLEXIONS SUR LES TECHNIQUES DE SIMULATION

Il est évident que disposer d'un outil reproduisant fidèlement le comportement d'un système peut apporter beaucoup aux concepteurs et utilisateurs.

L'outil le plus fidèle est le système lui-même. Ceci justifie la construction de prototypes. Mais il est évident qu'un prototype coûte cher, qu'il arrive tard après qu'aient été faits des choix quasi-irréversibles, qu'il ne peut, sans risques excessifs, pour le matériel et pour le personnel, être poussé aux limites du domaine d'utilisation.

Un prototype trouve sa justification, ce n'est pas le lieu ici d'en discuter. Il n'en reste pas moins qu'il est très utile de disposer le plus tôt possible de systèmes simulant le système réel.

Les développements de l'informatique fournissent des solutions qui révolutionnent les méthodes de conception traditionnelles.

Le DAO (Dessin Assisté par Ordinateur) permet de "voir" le système en trois dimensions bien avant la réalisation d'une maquette. Une maquette est un simulateur puisqu'il simule l'occupation spatiale du système réel. Le DAO est également un outil de simulation, puisqu'il permet d'essayer diverses solutions géométriques ou cinématiques. La CAO (Conception Assistée par Ordinateur), en général associée au DAO, permet de soumettre, par le calcul, le futur système à des efforts mécaniques et des contraintes thermiques. Là encore, nous disposons d'un moyen permettant des décisions précoces avant de disposer de banc d'essais de charges statiques et thermiques, de fatigue mécanique et thermique, bancs qui eux aussi peuvent être considérés comme des simulateurs.

Grâce à l'informatique, il est enfin possible de représenter, plus ou moins fidèlement, l'évolution dans le temps des paramètres caractéristiques d'un système en réponse à des variations de commandes ou des sollicitations de l'environnement.

Ce sont ces systèmes que l'on appelle en général des simulateurs, bien que la simulation, nous venons de le voir, recouvre un domaine plus vaste.

Mais ce terme de simulateur, même employé avec cette signification restrictive de simulateur de fonctionnement, couvre en réalité des systèmes répondant à des objectifs très différents. Cela conduit à des confusions fâcheuses dans la conception et l'utilisation de ces systèmes, par confusion sur les tâches à leur confier.

LES DIFFÉRENTES CLASSES DE SIMULATEUR.

Nous distinguerons deux grandes classes de simulateurs de fonctionnement:

- les Simulateurs de Comportement Système qui ont pour tâche
  - la compréhension des phénomènes physiques expliquant le comportement du système à étudier,
  - l'exploration des limites du domaine d'utilisation sûr en cas d'événements perturbateurs rares, difficiles et dangereux à essayer sur le système réel.
  - le comportement accidentel au-delà des limites.
- les Simulateurs d'Interface Homme - Machine qui ont pour objet l'étude du comportement des opérateurs face au nouveau système. Ces simulateurs se divisent encore en deux sous classes
  - les simulateurs d'étude destinés à concevoir la meilleure interface (disposition des instruments et des commandes),
  - les simulateurs d'entraînement destinés à la formation des futurs opérateurs ou au maintien des connaissances des opérateurs en service.

Les objectifs étant différents, les caractéristiques générales de conception de ces machines sont différentes.

LES MODÈLES MATHÉMATIQUES.

Les Simulateurs de Comportement Système doivent comporter des algorithmes serrant au plus près la réalité physique. Ainsi un échangeur doit-il être représenté par l'ensemble des équations traduisant le plus fidèlement possible les échanges thermiques et les écoulements hydrodynamiques dans les canalisations. Les algorithmes sont alors des "modèles de connaissance". Bien entendu chaque modèle de connaissance a ses limites de validité et utilise, sans le dire, des modèles dits de "représentation", qui ne font que représenter le phénomène physique sans l'expliquer. C'est ainsi que les écoulements hydrodynamiques sont représentés par des lois empiriques traduisant l'évolution des pressions par des "pertes de charges" réparties le long des canalisations. En réalité ces lois empiriques ne font qu'utiliser les résultats que l'on pourrait obtenir en intégrant les équations de Navier. Ces mêmes équations considérées comme un modèle de connaissance reposent sur des considérations macroscopiques traduisant, statistiquement, le comportement du fluide à l'échelle moléculaire. Elles reposent ainsi sur des modèles de représentation, sous-jacents, par exemple le modèle des forces de viscosité.

Ainsi les Modèles Mathématiques des Simulateurs de Comportement Système sont-ils bâtis en utilisant des algorithmes choisis pour fournir au mieux la réponse du système à des sollicitations, dans un domaine de validité qu'il importe de bien identifier, domaine d'autant plus large que les modèles utilisés sont plus des modèles de connaissance que des modèles de représentation. Mais il faut prendre garde à ce qu'un modèle ne donne jamais le comportement réel dans tous les cas.

Utiliser des modèles de connaissance de plus en plus fouillés augmentera le domaine de validité, mais augmentera par la même occasion la complexité et donc le temps de calcul. Un compromis est nécessaire entre domaine de validité et temps de calcul (et nous ne parlons pas du risque d'erreur de logiciel qui croît lui aussi avec la complexité des modèles).

Il est donc fondamental, au moment de la conception d'un Modèle Mathématique, de se poser la question de l'amplitude nécessaire et suffisante du domaine de validité, fonction des objectifs fixés aux études utilisant ce modèle.

Il se peut que simuler un échangeur par un modèle de représentation simple soit largement suffisant si l'on est sûr de ne pas avoir à faire face à des situations simulées hors du domaine de validité du modèle. On peut ainsi utiliser une simple table donnant les deux températures de sortie en fonction des débits et des températures d'entrée et représenter les transitoires par des réponses du premier ordre entre valeurs initiales et valeurs finales fournies par la table. Mais il est évident que ce modèle ne permettra pas d'étudier des cas d'obstruction ou de rupture de canalisations de l'échangeur.

Ces mêmes considérations sont valables pour les Modèles Mathématiques utilisés pour les Simulateurs d'Interface Homme - Machine. Il faut là aussi se poser le problème du domaine de validité nécessaire et suffisant.

Très souvent des modèles de représentation simples, déduits de calculs faits à l'aide des Simulateurs de Comportement Système, peuvent se révéler largement suffisants. Il s'agit en effet d'étudier le comportement de l'opérateur face au tableau d'instruments et de commandes. Il suffit que l'évolution des paramètres, suite aux actions de l'opérateur, soit réaliste et non pas fidèle à la troisième décimale. Sauf cas particulier, le comportement de l'opérateur ne sera pas changé si l'équilibre attendu est obtenu en deux minutes trente au lieu des deux minutes vingt-huit données par le calcul du Modèle Mathématique sophistiqué du Simulateur de Comportement Système.

Il est par contre beaucoup plus important que le "tableau de bord" soit aussi proche que possible de la réalité, condition qui est en général sans intérêt pour le Simulateur de Comportement Système. L'objectif du Simulateur de Comportement Système est en effet de connaître la réponse précise du système à des sollicitations précises. Il faut donc introduire des entrées programmées et enregistrer les réponses et non pas introduire des entrées mal définies, comme celles produites par un opérateur, et se contenter de "voir" la réponse sur les instruments.

Nous voyons ainsi se dessiner les différences fondamentales entre les deux grandes familles de simulateur.

- un Simulateur de Comportement Système doit être constitué autour d'un logiciel sophistiqué (qui n'est pas obligé de fournir les réponses en temps réel) avec des entrées préprogrammées et des sorties enregistrées pour études ultérieures.
- un Simulateur d'Interface Homme - Machine doit être bâti autour d'un logiciel simple, travaillant nécessairement en temps réel, avec une représentation aussi fidèle que possible de l'interface.

En conséquence, il est néfaste d'essayer de bâtir un Simulateur universel répondant aux deux objectifs, sous peine de surdimensionner inutilement le système.

LES SIMULATEURS D'INTERFACE HOMME - MACHINE.

Revenons maintenant aux objectifs des simulateurs d'interface homme - machine.

Les simulateurs d'étude.

Un simulateur d'étude a pour objet de définir, le plus tôt possible au cours de la conception, l'interface la mieux adaptée aux opérateurs.

Le logiciel doit être capable de représenter le fonctionnement normal du système, ainsi que son comportement dans un certain nombre de cas incidentels typiques. Il n'est pas nécessaire toutefois de représenter le comportement accidentel, c'est-à-dire une fois dépassées les limites de fonctionnement sûr. Il ne s'agit pas, par exemple, de voir l'évolution des paramètres une fois déclenchée la fusion du cœur d'une centrale nucléaire ou une fois dépassée l'incidence de décrochage d'un avion de ligne. Ce problème n'est pas celui de l'interface homme - machine (ce peut être par contre celui du Simulateur de Comportement Système, dans la mesure où les connaissances actuelles permettent une modélisation valable).

L'interface homme - machine, visualisation du monde extérieur, panneaux d'instruments, écrans, commandes doit être représentée avec réalisme et surtout doit pouvoir être modifiée souplement, car il s'agit, non pas de vérifier la validité d'une disposition connue, mais d'essayer diverses solutions. Il faut savoir en effet que généralement les solutions envisagées sur la planche à dessin n'apparaissent pas toujours optimales une fois présentées aux opérateurs. De nombreuses retouches, quelque fois de détail, sont souvent nécessaires. Il ne faut pas qu'une modification de l'interface se traduise par des jours de travail de découpage de tôle et de câblages.

Nous avons dit que l'interface devait être réaliste. Cela ne veut pas dire strictement conforme à la réalité. La forme précise d'un inverseur importe peu. Il suffit que l'inverseur utilisé entre dans la gamme des manipulateurs connus de l'opérateur. C'est sa position sur le tableau et son sens de manipulation qui sont importants à tester plutôt que sa forme. Bien sûr la forme devra être étudiée, mais dans un second stade seulement.

De même la technologie des écrans n'est pas fondamentale, ce sont les paramètres qui y sont présentés, leur type de présentation (analogique, numérique, courbes, diagramme) qui sont importants à définir. Bien entendu il ne faut pas utiliser un écran texte noir et blanc pour simuler un écran graphique couleur haute définition, mais la taille et la qualité de l'écran ne sont pas fondamentales à ce stade de l'étude.

A cette occasion il est bon de noter qu'une étude préalable sur "maquette informatique" doit permettre de défricher un certain nombre de points avant d'essayer la solution sur simulateur (c'est ce que nous avons appelé les micro-simulateurs au chapitre précédent). Il n'est en effet pas nécessaire de disposer de la réponse réelle du système pour estimer la qualité d'une présentation d'information ou d'une disposition de commande. Il suffit souvent de bâtir une maquette animée sur micro-ordinateur pour juger la validité d'une solution. Le choix par exemple entre une présentation digitale ou analogique, la taille des caractères, la précision et l'orientation (verticale ou horizontale) des échelles, le libellé, la taille, la couleur, la position sur écran des messages, etc. peut se faire sur une maquette animée par un petit programme très simple. C'est la solution ainsi définie qui sera validée ultérieurement sur simulateur, puis sur prototype, avec de meilleures chances de succès rapide.

En définitive, un Simulateur d'Étude de l'Interface Homme - Machine doit répondre aux critères minimaux suivants

- posséder un logiciel aussi simple que possible donnant des réponses réalistes aux sollicitations et capable de simuler les principales situations incidentelles, car la définition de l'interface doit se faire en prenant également en compte le fonctionnement anormal.
- être bâti autour d'un tableau de bord réaliste facilement modifiable.

Les simulateurs de formation.

Un simulateur de formation doit répondre à d'autres exigences, car ses objectifs sont différents.

Quelques considérations sur les objectifs et méthodes de formation doivent être développées au préalable.

Les opérateurs de systèmes complexes ne sont plus en contact direct avec la machine comme nous l'avons vu tout au long des chapitres de cet ouvrage. Ils doivent travailler à l'aide de modèles de représentation mentaux traduisant en "images", plus ou moins proches de la réalité, les informations dont ils disposent sur le tableau de bord ou provenant du "monde".

L'élaboration des stratégies et tactiques nécessite la connaissance correcte de l'état réel du système. Or cette connaissance, sous forme d'une image dans le cerveau de l'opérateur, repose sur deux types fondamentaux de prise d'information,

- la "lecture" d'un certain nombre de paramètres caractéristiques,
- la connaissance des événements antérieurs.

Ainsi l'image mentale de l'opérateur peut être faussée pour deux raisons,

⇨mauvaise interprétation des lectures, dont les causes sont légions

- non lecture par suite d'une surcharge de travail ou par manque de vigilance,
- erreur de localisation de la source d'information,
- erreurs instrumentales,
- brouillage (transmissions d'informations orales dans une ambiance sonore importante ou mauvais éclairage d'un instrument),
- erreur de zéro, d'échelle, etc.

Ces erreurs ont été abondamment décrites aux chapitres 2 à 6.

⇨ mauvaise interprétation des événements antérieurs, dont les raisons sont nombreuses également

- l'action précédente était une commande mal exécutée (erreur de commande, erreur de sens d'action de la commande, panne de la commande, etc.). L'opérateur croit alors que le résultat attendu a été obtenu et il ne le vérifie pas.
- deux événements, bien d'indépendants, se sont produits de façon concomitante (par exemple, ouverture d'un disjoncteur au moment de la mise en service d'un système hydraulique totalement indépendant). L'opérateur leur attribue une relation de cause à effet ce qui le conduit à "inventer" un modèle explicatif aberrant.
- la stratégie élaborée est une stratégie classique qui est efficace dans 99% des cas. Dans le cas, rare, où elle est inefficace, voire néfaste, l'opérateur l'applique sans vérifier le résultat qui ne fait pas de doute pour lui ou l'applique et ne comprend plus le déroulement des événements, aberrants pour lui. Il s'explique la situation en inventant des pannes et son modèle mental devient de plus en plus inadapté. Ce type d'erreur peut se produire lorsque l'opérateur, mal formé, s'est bâti un mauvais modèle de comportement du système, par exemple en généralisant abusivement une règle empirique qui ne s'applique que dans certains cas.
- des automatismes ont fait évoluer l'état à l'insu de l'opérateur, qui dès lors ignore cette suite d'événements et ne les prend pas en compte dans l'évolution de son image mentale du système.
- l'opérateur refuse de croire les informations qui lui sont présentées (alarmes interprétées comme une panne du système d'alarme lui-même, valeur "anormale" indiquée par un instrument interprétée comme une panne de capteur, etc.), car contraires à ce qu'il attendait compte tenu des événements précédents.
- etc.

Là encore ce type d'erreur a été largement décrit.

L'élaboration d'une mauvaise image mentale conduit à une erreur de représentation ou à une Conscience Erronée de la Situation.

La lutte contre les erreurs de représentation passe par des améliorations technologiques, fiabilité des capteurs, amélioration des instruments (éclairage, homogénéisation des zéros et des échelles, répartition spatiale des informations, hiérarchisation des alarmes évitant l'effet "arbre de Noël"...), disposition des commandes, etc. C'est l'un des rôles des simulateurs d'étude que d'aider au choix des meilleures solutions en la matière.

La formation est également un outil de lutte contre les erreurs de représentation.

La formation permet en effet d'atteindre une connaissance détaillée du tableau de bord, c'est-à-dire des instruments, de leur disposition, de la signification et du rôle de chaque paramètre, de la disposition et du sens d'action et du rôle des commandes. Un entraînement au simulateur permet "d'automatiser" les opérations les plus courantes et de mettre en mémoire les modèles de localisation et de vérification des sources d'information, les modèles d'interprétation des informations ainsi que les modèles de localisation, de vérification et de sens d'action des commandes. Nous reviendrons sur les caractéristiques nécessaires d'un bon simulateur répondant à cet objectif.

La lutte contre les erreurs dues à une Image a priori ou à l'utilisation d'un mauvais modèle de risque est beaucoup plus délicate.

Plusieurs stratégies ont été proposées. Elles ne sont pas concurrentes mais, à notre avis, complémentaires.

L'une des stratégies repose sur la formation. Nous ne citerons que celle là, les autres sortant du cadre de ces réflexions sur les simulateurs (approche par état, systèmes de détrompage, chapitre 12).

Généralement les opérateurs ignorent l'existence même des erreurs de représentation. Les incidents ou accidents dont ces erreurs sont la cause, sont très souvent interprétés, une fois les événements "décortiqués", comme résultant de l'incompétence de l'opérateur: "ce n'était pourtant pas difficile de détecter l'existence d'une petite brèche dans le primaire, il y avait 19 paramètres dont les valeurs anormales pouvaient alerter l'opérateur! (accident de la centrale nucléaire de Three Mile Island)".

Il est donc important de faire connaître ce type d'erreur aux opérateurs en leur en signalant l'existence par des présentations théoriques et en les mettant en évidence par des analyses d'incidents réels.

Mais il est également nécessaire de mettre les opérateurs, au simulateur, dans des situations d'erreur de représentation, pour leur montrer que cela n'arrive pas qu'aux incompétents. Ce type d'expérience, entamée dans l'aéronautique a déjà porté ses fruits en permettant à des équipages de prendre conscience de la réalité du phénomène (expérience ARCHIMEDE, voir Chapitre 8).

Ces quelques rappels sur les problèmes d'erreur d'opérateurs étant faits, revenons au problème particulier des simulateurs de formation.

Rappelons que former c'est fournir les bons modèles d'action et les bonnes images mentales permettant une analyse correcte des situations.

Convaincre quelqu'un ne consiste pas à lui imposer, brutalement, ses propres conclusions. Cela consiste à l'amener, de lui-même, aux mêmes conclusions, en l'aidant à formuler un raisonnement analogue.

De même former quelqu'un ne consiste pas à lui imposer brutalement les théories, les modèles et les images. Cela consiste à l'amener, de lui-même, à se forger les bons modèles à partir de sa propre expérience. Le formateur n'est là que pour guider c'est-à-dire indiquer le bon chemin et redresser les erreurs.

La simulation est l'un des moyens d'acquisition des bons modèles par l'expérience personnelle, à condition de disposer d'un formateur qui surveille en permanence les opérations de formation et contrôle la "naissance" des images mentales et des modèles dans le cerveau de l'opérateur pour éviter au mieux les déviations.

Les opérations de formation nécessitent, outre les moyens audiovisuels classiques, des moyens de simulation qui là encore doivent être adaptés au but recherché.

LES DIFFÉRENTS TYPES DE SIMULATEURS DE FORMATION.

Nous distinguerons quatre types de simulateurs de formation.

⇨ Les simulateurs destinés à faire comprendre la physique des phénomènes rencontrés.

Il s'agit de faire effectuer aux opérateurs des "travaux pratiques" peu coûteux, disponibles en salle et sans danger pour le matériel et le personnel. Ce sont des simulateurs en ce sens qu'ils sont interactifs. L'opérateur manipule lui-même pour observer le résultat de ses actions. Il n'intervient pas au moyen des commandes classiques, mais il fait varier des paramètres d'environnement, programme des entrées, etc. pour voir comment évolue le système dans ces conditions.

Par exemple, il dispose d'un modèle de fonctionnement du pressuriseur d'un réacteur nucléaire et peut faire varier le volume et la température du fluide primaire, la température du pressuriseur. Agissant sur les chaufferettes (dont il peut régler l'allure) ou la douche (dont il peut régler le débit et la température), il peut examiner comment évolue la pression. Les commandes, on le voit, sont artificielles, mais l'opérateur peut ainsi acquérir le modèle physique correct de fonctionnement du pressuriseur et comprendre les lois qui le régissent.

De tels simulateurs nécessitent des logiciels relativement simples, reposant sur des modèles de connaissance et quelquefois sur des modèles de représentation.

Les commandes à la disposition des opérateurs sont le clavier et la souris, en prenant garde à ce que la manipulation soit la plus simple possible. L'informatique doit être complètement transparente pour l'opérateur. Il ne faut pas qu'il soit bloqué par un apprentissage fastidieux du système informatique.

Enfin les résultats doivent être présentés sous forme d'images schématisant la réalité, de façon à faciliter la formation des bonnes images mentales. On peut y adjoindre des courbes et des diagrammes dans la mesure où ce type de présentation s'avère strictement nécessaire à la compréhension des phénomènes.

Ainsi dans notre exemple on présentera une vue en coupe simplifiée du pressuriseur, avec une représentation du niveau, un manomètre et un thermomètre. On peut à l'occasion de certains essais et dans un deuxième temps, montrer en outre les évolutions du point de fonctionnement, pression, température sur un diagramme où figure la loi de pression de vapeur saturante ou représenter les évolutions de la pression et de la température en fonction du temps.

⇨ Les simulateurs destinés à se mettre en tête

- la répartition spatiale des instruments, les paramètres représentés, les échelles, les zéros (modèles de localisation et de vérification des sources d'information et modèles de transposition des informations),
- la répartition spatiale des commandes, leur rôle, leur sens d'action (modèle de localisation et de vérification des commandes, modèles d'action des commandes),
- la répartition spatiale et la signification des alarmes,
- les opérations de manipulation du tableau de bord, éclairage, verrouillage et déverrouillage des commandes, manipulation des caches de protection, manœuvre des écrans cathodiques, des systèmes de changement d'échelles, connaissance des claviers et rôle des touches, etc.

De tels simulateurs peuvent se réduire à des maquettes fixes, mais il est fructueux de les animer quelque peu. En particulier, les commandes d'écran doivent s'accompagner de présentations d'information réalistes, permettant une manipulation proche du réel. Il faut avoir vu l'effet de telle commande d'appel d'un diagramme pour mémoriser facilement le mode opératoire.

Il peut sembler luxueux de disposer de tels simulateurs et penser qu'il est moins onéreux d'utiliser le simulateur complet d'entraînement pour ce type de formation. C'est un bilan à faire, mais en général les simulateurs d'entraînement sont saturés et il n'est pas, en outre, toujours facile de pouvoir montrer toutes les manipulations possibles sur un simulateur en fonctionnement car l'on y est tributaire des opérations simulées en cours. Par ailleurs il est indispensable que les opérateurs soient parfaitement au fait des divers modes opératoires du tableau de bord pour profiter au mieux des leçons de l'expérience au simulateur complet. Les conséquences de l'apparition d'une brèche au primaire et les consignes à appliquer seront ignorées de l'opérateur perdu dans la manipulation chaotique de son écran de contrôle!

⇨ Les simulateurs destinés à comprendre le fonctionnement d'un sous système particulier. Ce type de simulateur est en général nommé simulateur de fonction.

C'est un système intermédiaire entre le premier et le dernier type. On est proche du simulateur complet, mais seule une ou quelques fonctions sont simulées.

Le logiciel est évidement plus simple que celui du simulateur complet, encore que la représentation de l'interface avec les autres systèmes ne soit pas toujours simple. L'interface avec l'opérateur peut également être simplifiée puisque seules quelques fonctions sont simulées.

Dans certains cas, l'interface avec l'opérateur peut être réduite à un simple écran où sont représentées sur plusieurs "pages" facilement manipulables, les informations et les commandes. C'est ainsi que nous avons pu réaliser, sur micro-ordinateur, un simulateur de la fonction RCV (contrôle volumétrique et chimique) d'un REP 900 MW d'EDF. Le tableau de commande occupait 24 pages d'écran, le tableau d'instruments 18 pages et le tableau d'alarmes 5 pages. Chaque page pouvait être rapidement appelée en désignant, avec le pointeur de souris, la partie de pupitre concernée sur un schéma général. L'expérience a montré qu'après une ou deux séances d'un quart d'heure les opérateurs oubliaient l'aspect manipulation du simulateur lui-même pour se consacrer aux problèmes spécifiques du RCV simulé. Ce simulateur, qui a été achevé il y a près de vingt ans, ne bénéficiait que des techniques d'écrans CGA (320 x 200 pixels en 4 couleurs). Il est évident que les écrans actuels (1500 x 900 pixels ou plus, de 256 à près de 17 millions de couleurs) facilitent les problèmes d'imagerie, comme en témoignent les simulateurs de démonstration que nous avons récemment réalisés.

L'avantage de tels simulateurs est de permettre de focaliser l'attention de l'opérateur stagiaire sur la seule fonction simulée sans se soucier du fonctionnement d'ensemble. L'acquisition des bonnes images mentales et des manipulations réflexes s'en trouve dès lors facilitée parce que plus simples et moins nombreuses à mémoriser.

⇨ Les simulateurs destinés à comprendre le fonctionnement du système complet.

La caractéristique essentielle d'un tel simulateur est de posséder une interface homme - machine identique à l'interface réelle.

Pour qu'une simulation soit parfaite, il faut :

- que la tâche imposée à l'opérateur soit identique à la tâche réelle (*identité de tâche*),
- que l'opérateur dispose de moyens d'actions identiques sur le système simulé et sur le système réel (*identité de commandes*).
- que l'opérateur dispose d'informations identiques sur l'état et l'évolution de l'état du système simulé d'une part, et sur l'état et l'évolution de l'état du système réel d'autre part (*identité d'informations*).

On constate rapidement que le meilleur simulateur est le système lui-même. Néanmoins la simulation, même avec quelques imperfections, s'impose :

- pour réduire les coûts. Même un calculateur très complexe coûte moins cher qu'un avion de ligne, une centrale nucléaire, un navire pétrolier, une motrice de TGV.
- pour réduire les risques d'expérimentations. Un crash à l'atterrissage, un arrêt d'urgence, un échouage, un freinage de détresse sont plus confortables au simulateur.
- pour augmenter la fréquence possible des expérimentations. Le calculateur peut en moins d'une seconde ramener l'avion simulé en position de début d'approche prêt pour un nouvel essai, alors que la même manœuvre réelle demande une dizaine de minutes pour être exécutée. Ramener le TGV Trans Manche à l'entrée du tunnel n'est pas simple autrement qu'au simulateur !
- pour permettre l'expérimentation dans des conditions extrêmes identifiables et reproductibles. Les turbulences extrêmes sont rares et si l'on veut entraîner les équipages d'avion de ligne dans ces conditions, on n'est jamais maître des états de l'atmosphère réelle.

Pour des raisons de coût et quelques fois pour des raisons de principe, il n'est pas toujours possible de satisfaire les trois critères d'identité de tâche, d'identité de commande, d'identité d'information.

Il peut sembler que le premier critère d'identité de tâche soit le plus facile à satisfaire. Il suffit de demander à l'opérateur de faire la "même chose", donc lui fixer les mêmes objectifs de mission.

En réalité, le problème se complique du fait que l'opérateur a bien souvent du mal à oublier qu'il travaille sur simulateur et que dans ces conditions les incidents les plus graves sont sans conséquences.

Nous allons voir que le respect des deux autres critères réduit l'ampleur du problème. Il est nécessaire néanmoins de rendre l'environnement de l'opérateur aussi réaliste que possible.

L'absence de certains détails que l'on ne pense pas toujours à reproduire, comme une légère vibration, un bruit de conditionnement d'air, un bruit de moteur, voire même une odeur, peut empêcher l'opérateur de "s'y croire". Seuls les opérateurs ayant une bonne expérience du système à simuler ou de systèmes analogues peuvent signaler les détails à ne pas oublier. Si les opérateurs portent normalement en service une tenue spéciale, uniforme par exemple, il est important qu'ils la portent en simulation. Il est stupide de gâcher une séance de simulation par une sonnerie intempestive de téléphone ou l'intrusion d'une personne étrangère à l'action simulée.

En outre seuls les mêmes opérateurs, par souvenir des conditions réelles, peuvent recréer les conditions psychologiques leur permettant d'oublier qu'ils sont sur simulateur.

Ainsi un pilote chevronné "ressentira" les accélérations sur un simulateur d'avion, sans reproduction du mouvement cabine, parce que, par réflexes acquis en vol, il contractera ses muscles abdominaux sur informations d'évolutions de l'avion, provenant de la visualisation du monde extérieur et de ses actions sur les commandes. Par contre un opérateur ignorant tout du vol réel ne ressentira rien. Une solution retenue sur les simulateurs d'avion à base fixe consiste à gonfler un coussin sur le siège pilote au

moment des accélérations. Si le pilote est soigneusement sanglé sur le siège, l'augmentation de la réaction du siège sur son corps lui suggère l'augmentation de son poids apparent lors d'une évolution et l'aide à recréer psychologiquement l'ensemble des sensations perçues dans ces conditions (il est impossible de reproduire la sensation désagréable produite par le mouvement des joues et du menton attirés "vers le bas" au cours d'un virage serré !).

Par ailleurs, un opérateur ignorant la conduite réelle du système risque d'utiliser les petits défauts de la simulation comme informations complémentaires, parce qu'il ne les identifie pas comme étant des défauts. On peut ainsi voir des techniciens chargés d'un système de simulation, mais ignorant la conduite réelle, faire preuve d'une dextérité vexante pour les opérateurs chevronnés. En réalité, ils pilotent un autre système que le système réel avec des informations qui n'existent pas dans la réalité et que les pilotes confirmés ne pensent même pas à utiliser.

Ces remarques font ressortir le fait que l'on ne doit pas espérer faire apprendre à piloter sur un simulateur. Il est par contre possible de "transformer" un pilote sur un nouvel avion. Dans ce cas, le pilote connaît les procédures générales et les ambiances réelles. Il ne reste qu'à lui apprendre les particularités de la machine qu'il ne connaît pas encore. Il peut ainsi apprendre les procédures, les "mécaniser" et les comprendre. Mais un débutant ne pourra acquérir sur simulateur ce que l'on appelle le "sens de l'air", c'est-à-dire la connaissance des conditions réelles d'ambiance du vol et des réflexes élémentaires de pilotage.

Ainsi un simulateur peut-il aider un pilote confirmé à connaître les particularités d'un nouveau système et à s'entraîner à l'application de procédures particulières. Dans le cas d'un simulateur d'entraînement, il est donc recommandé de s'appliquer à reproduire fidèlement la disposition des commandes et des instruments de contrôle pour que l'opérateur puisse acquérir les "automatismes" valables pour le réel. Par contre, un simulateur didactique destiné à faire comprendre le rôle et le fonctionnement des systèmes peut être moins fidèle. Il s'agit de comprendre intellectuellement avant d'acquérir les automatismes.

Rendre les commandes aussi réalistes que possible est certainement le critère le plus facile à respecter.

Il faut toutefois distinguer les différents types de simulateurs. Pour un simulateur d'entraînement, nous venons de le voir, il est indispensable de respecter strictement les formes et la disposition des commandes. Il s'agit, en effet, de faire acquérir à l'opérateur les modèles corrects de localisation des commandes et de mode d'action des commandes. Par contre pour les simulateurs d'étude et les simulateurs didactiques le respect du critère d'identité des commandes peut être plus lâche. Il suffit que les commandes soient d'un modèle réaliste.

Les informations fournies par les instruments sont très faciles à reproduire. Le problème est beaucoup plus délicat en ce qui concerne les informations provenant de l'environnement pour les simulateurs de véhicules. Or une grande partie des informations nécessaires au pilotage provient du monde extérieur, qu'il convient donc de représenter.

De nombreuses solutions technologiques sont disponibles lorsqu'il s'agit de représenter ce que l'opérateur observe du monde extérieur, projection sur écran d'images prises par une caméra se déplaçant par rapport à une maquette, projection d'images synthétiques calculées en temps réel, etc. Cette dernière solution a fait ces dernières années des progrès décisifs et elle supplante désormais la première. Tous ces dispositifs ne fournissent en général qu'une vision sans relief, ce qui est suffisant pour simuler la vision d'un paysage relativement éloigné. Le déplacement relatif des objets suffit pour restituer l'impression de relief. Par contre, lorsqu'il s'agit de représenter le champ visuel proche, l'absence de relief est très nettement ressentie et peut perturber l'opérateur. Des progrès restent à faire dans ce domaine, mais des solutions sont à l'étude, de moins en moins coûteuses sur le plan du matériel et amortissables pour le logiciel, si les pratiques de simulation se généralisent.

La représentation des forces d'inertie pose un problème de principe impossible à résoudre. Seule la reproduction de la trajectoire réelle permettrait de faire subir les forces d'inertie réelles à l'opérateur. Il semble heureusement que l'homme soit plus sensible aux variations des forces d'inertie qu'aux forces d'inertie elles-mêmes.

Ainsi avec des mouvements d'amplitudes limitées, il est possible de rendre compte de ces variations. Les mouvements de la cabine du simulateur sont ceux de la machine à simuler, filtrés par un filtre passe-haut, le retour en position moyenne étant assuré par des mouvements dont les accélérations sont inférieures au seuil de perception de l'opérateur. Il est par ailleurs possible de "représenter" les facteurs de charge continus, du moins normaux à la trajectoire, par un gonflement du coussin de siège, nous l'avons déjà vu et les variations de direction de la verticale apparente par des mouvements de la cabine autour de la verticale, tout en laissant la visualisation de l'extérieur fixe par rapport à la cabine. Il est ainsi possible par de multiples "astuces" de tromper l'opérateur et lui fournir un succédané de sensations, qu'il identifie, "psychologiquement", aux sensations réelles, s'il connaît bien l'environnement naturel du véhicule.

Les considérations que nous venons de développer relèvent du bon sens. Il est fondamental de ne pas oublier l'objectif de la simulation projetée.

Un simulateur d'entraînement doit permettre à l'opérateur de bâtir solidement ses modèles de représentation personnels. Il importe donc de l'aider dans cette tâche et faire en sorte de ne pas fausser la représentation et risquer de le conduire vers des modèles faux. En particulier le logiciel doit pouvoir non seulement présenter le fonctionnement normal du système mais également le fonctionnement dans les cas des incidents fréquents caractéristiques. Un tel simulateur ne peut généralement pas être bâti sur micro-ordinateur surtout lorsque le système doit être piloté par une équipe sauf pour les petits systèmes (on retrouve alors les caractéristiques des simulateurs de fonction).

LES ESSAIS AU SIMULATEUR.

Il nous reste maintenant à interpréter les essais effectués soit au simulateur, soit sur le véhicule ou sur le système réel.

Les estimations de la charge de travail.

Les méthodes d'évaluation de la charge de travail sont évoquées dans l'annexe 3. Nous y renvoyons le lecteur.

Les études d'erreurs de représentation.

La notion d'erreur de représentation est encore trop récente pour que de nombreux essais aient déjà été entrepris sur le sujet. Il est évident que l'observation directe et objective de l'ensemble opérateur-système ne peut en aucun cas fournir la moindre indication puisque tout se passe dans la tête de l'opérateur !

Néanmoins des opérateurs, bien au courant du problème des erreurs de modèles, peuvent, après essais, dresser la liste des problèmes rencontrés et des erreurs potentielles, erreurs possibles sur les modèles de localisation des sources d'information et des commandes, sur les modèles de mode d'action des commandes et d'interprétation de l'information. Un tel résultat était déjà obtenu sur avion avec les études cabine, mais la notion d'erreur de modèle étant ignorée, un certain flou existait sur les raisons qui faisaient que l'opérateur émettait des critiques. On peut maintenant espérer une certaine organisation de recherche des erreurs possibles. Les notions de modèles de conduite, de pilotage, de commande, de fonctionnement, de configuration peuvent également aider à organiser la critique.

Enfin l'observation des opérateurs en cours de travail peut aider à détecter les conditions potentielles d'entrée dans les erreurs de représentation et surtout les raisons de sortie d'erreur. Le vrai problème est la recherche des conditions physiques et psychologiques qui conduisent l'opérateur à se frapper le front et s'écrier "Bon Sang, mais c'est bien sûr!".

Il est évident que l'observation est très délicate car elle risque de troubler l'opérateur. Par ailleurs, on voit difficilement l'observateur demander à l'opérateur en cours d'essai s'il croît être en erreur de représentation ! On tombe sur toutes les difficultés bien connues des études de psychologie expérimentale.

Actuellement, les recherches de méthodes expérimentales s'orientent vers l'enregistrement aussi fidèle que possible des actions de l'opérateur. La séance de simulation est alors rejouée devant l'opérateur, sur le simulateur

lui-même, le plus tôt possible après l'essai. On lui fournit le maximum de renseignements sur son comportement ; par exemple on lui signale, en temps réel, sur quels instruments ou commandes se portait son regard, quelles commandes ont été manipulées, etc. Il est alors possible de l'interroger sur le contenu de ses pensées à chaque instant, en espérant que le déroulement des événements sous ses yeux lui permettra de se remémorer ce qu'il avait en tête à ces instants. L'expérience montre d'ailleurs que bien souvent l'opérateur est très étonné de voir en détail la succession des opérations qu'il a effectuées quelques instants avant; il en avait gardé un souvenir très différent (c'est d'ailleurs l'une des origines des erreurs de représentation).

On consultera le Chapitre 8 donnant quelques détails des opérations ARCHIMEDE (Action de Recherche sur le Comportement Humain en Incident. Méthode d'Évaluation et de Détection des Erreurs) consistant à faire exécuter, à des équipages entraînés, des vols simulés reproduisant des conditions accidentogènes tirées de l'exploitation d'accidents réels.

CHAPITRE 14

La Morale et le Droit, hérités de la sagesse des Anciens, nous imposent de punir fermement toutes les erreurs sauf une, l'erreur judiciaire.
Miss Anne Hexamin

SECURITE ET RESPONSABILITE PENALE

L'abondante littérature traitant des problèmes de sécurité montre la grande difficulté que rencontre la justice lors de la détermination des responsabilités, à l'occasion d'accidents intervenant dans les systèmes industriels complexes. On y constate combien il est injuste de ne retenir que la responsabilité de l'agent qui a directement été la cause d'un dommage et nous partageons totalement ce point de vue. Nos études des accidents, dans le domaine des industries de production et dans le domaine des transports, nous ont en effet montré à l'évidence qu'un accident est dû à une succession malheureuse d'événements et que le dernier ne peut pas être considéré comme la cause de la catastrophe, de préférence à l'un quelconque des autres événements. Il suffit qu'un seul des événements de la chaîne n'ait pas lieu pour que l'accident soit évité.

Pour bien analyser un accident afin de trouver des remèdes ou des parades pour le futur (c'est l'un des rôles des techniciens chargés de la sécurité) il est presque toujours nécessaire de remonter loin en amont de l'événement final pour établir, en essayant d'atteindre l'exhaustivité, la chaîne d'événements, ayant conduit à la catastrophe. On constate alors bien souvent, en particulier lors de l'analyse des grandes catastrophes, que chaque événement de la chaîne, ainsi reconstituée, est d'une grande banalité, et s'est déjà produit de nombreuses fois sans conséquence. On constate également que ces événements appartiennent à des domaines très divers et résultent de problèmes d'organisation générale de l'entreprise, des règles d'entretien et de maintenance du matériel, des méthodes de conception des matériels et des interfaces homme-machine, des procédures d'emploi et de conduite, etc. Si nous soulignons ce fait, ce n'est en aucun cas pour rejeter la notion de responsabilité, comme on nous le reproche souvent, mais pour mettre en évidence les grandes difficultés que la justice rencontre à trouver "le seul et unique responsable" de tous ces événements. Généralement des erreurs (ou des fautes) ont été commises par des opérateurs, c'est exact, mais également par les concepteurs, les autorités responsables de la sécurité, les compagnies exploitantes, etc. !

Il est pour nous évident que toute faute mérite sanction, dans la mesure où la faute est réellement établie. Ainsi le responsable d'un système de transport de passagers ou de fret qui, par des dispositions d'organisation interne, oblige ses opérateurs, conducteurs ou pilotes, à exécuter des opérations au-delà des durées légales du travail, le responsable d'une unité de production qui néglige, volontairement, dans un souci illégitime de productivité, les règles élémentaires de sécurité, doivent être sanctionnés au même titre que le conducteur qui roule à 200 km/h ou qui double en haut de côte. La faute est dans ces divers cas, évidente, indépendamment des conséquences et nous estimons que la sanction doit être aussi lourde que ces manquements patents aux règles élémentaires de sécurité aient été suivis ou non de conséquences graves (mais ceci est un autre problème !).

Notre propos n'a pas pour objet de prôner une politique de laxisme à tout prix dans la recherche des responsabilités en matière d'accidents industriels en transformant toute faute en erreur, loin de là. Nous voulons seulement montrer que l'application brutale de l'article 212-6 du Code pénal peut conduire à transformer toute erreur en faute, et dans quelques cas à transformer une démarche normale, tenant compte des impératifs de sécurité, en une faute, pour peu que s'en mêlent des circonstances, prévisibles peut-être, mais hautement improbables. C'est ainsi que le but de chaque analyse d'accident est d'en retrouver, dans la mesure du possible, toute la genèse et si des erreurs humaines sont détectées de rechercher si elles sont explicables par des erreurs de conception, ou d'organisation ou si elles sont réellement des fautes. Il est évident que condamner l'auteur d'une erreur due à une mauvaise conception du tableau de commande d'une machine n'empêchera pas un autre opérateur de commettre la même erreur. La punition n'aura d'effet que si une faute contre la discipline a été commise.

Donnons quelques exemples de cas concrets destinés, non pas à définir des responsabilités, mais à faire réfléchir les juristes avec nous, comme nous avons tenté de le faire lors de plusieurs colloques Juristes Ingénieurs à Bordeaux en 1991 puis à Lyon depuis 1993.

Les expériences ARCHIMEDE

Les opérations RACHEL, SEMIRAMIS et ARCHIMEDE, menées pour le compte de la Direction Générale de l'Aviation Civile, avaient pour objectif une meilleure compréhension du rôle des erreurs humaines dans la genèse des accidents aériens. Nous les avons décrites au chapitre 8, nous n'y reviendrons pas et rappellerons simplement les conclusions qui nous intéressent ici sur le plan juridique.

Les équipages ont tous reconnu que les scénarios étaient très conformes à la réalité d'un vol et qu'ils n'ont pas eu l'impression d'avoir été "piégés" par des événements anormaux que l'on ne peut rencontrer en vol.

Nous pensions observer une ou deux erreurs. Le résultat a été tout autre !

Chaque scénario a provoqué systématiquement, des déviations importantes proches de l'accident.

Les événements, dont la succession conduit à cette situation critique sont d'une extrême banalité (petites erreurs courantes commises très souvent mais la plupart du temps corrigées très rapidement ou sans conséquences dans le contexte et par suite rarement notées par les équipages).

C'est l'enchaînement malencontreux de ces erreurs qui est rare, mais non l'occurrence de chaque erreur.

Le rôle des scénarios était de provoquer cet enchaînement malencontreux en favorisant une erreur au mauvais moment ou en interdisant la correction par un événement extérieur, réaliste, judicieusement provoqué.

Ces résultats ont conduit à examiner un fichier analogue au fichier RACHEL mais répertoriant, non les accidents, mais les incidents graves.

Une analyse du fichier "Incidents" n'a pas fait apparaître de familles nouvelles. Les accidents ne seraient que des incidents qui ont "mal tourné", mais ne semblent pas être de nature différente. Ceci milite en faveur du recueil de ce type de données, car les incidents sont beaucoup plus fréquents que les accidents et plus facile à analyser, en particulier parce que l'équipage peut "s'expliquer". Malheureusement la tendance fâcheuse consistant à considérer que les erreurs sont des fautes rend encore difficile la divulgation de ces données fondamentales pour la sécurité. Nous avons évoqué ce problème dans le chapitre traitant du Retour d'Expérience.

Ce rappel "technique" des expériences ARCHIMEDE étant fait nous pouvons nous interroger sur les responsabilités des équipages, des compagnies aériennes et des concepteurs d'avions de ligne.

Si la grande majorité des équipages participant à l'opération, en conditions réalistes de simulation, mis dans les mêmes conditions, commet les mêmes chaînes d'erreurs conduisant à la catastrophe, on est en droit de se poser la question de la responsabilité des équipages qui ont été réellement impliqués dans les accidents. Sachant que les erreurs étaient toutes, prises séparément, extrêmement banales (et dans la plupart des cas normaux corrigées instantanément ou sans conséquences), on peut également se poser la question de la responsabilité des compagnies et des concepteurs.

Nous nous garderons bien de trancher, n'étant que techniciens et non juristes !

Il se peut, par ailleurs, qu'un opérateur se révèle par trop sujet à l'erreur. Ce cas est rare, car en général, ce genre de défaut est détecté au moment de la formation. Il peut arriver cependant, qu'un élève, brillant pendant la formation (c'est un fort en thème), soit incapable de prendre ses responsabilités, une fois plongé dans l'univers non protégé du réel. S'il n'est pas question, à notre avis, de le sanctionner pour ses maladresses ou ses erreurs, il n'en reste pas moins qu'il est du devoir de ses supérieurs de l'orienter vers d'autres tâches, surtout si ces erreurs compromettent la sécurité. Cette réorientation ne doit pas être considérée comme une sanction mais comme une opération de sécurité, au même titre que l'on changera d'affectation un opérateur devenu inapte pour des raisons de santé. Dans l'état actuel de notre morale il est remarquable de constater que l'on fera plus facilement accepter à la communauté et à l'intéressé un changement de poste pour raison médicale (la vision de nuit du conducteur s'est détériorée), que par suite d'une accumulation malheureuse d'incidents plus ou moins graves mettant en doute ses capacités de conduite. Le changement de responsabilité d'un opérateur mal adapté à sa tâche sera envisagé comme une sanction et non comme une opération de sécurité. Il est vrai que nous sommes considérés comme coupables de faire des "fautes" d'orthographe (qui ne sont que des erreurs bien involontaires car nous ne voyons vraiment pas à qui profite la faute !), alors que personne ne nous reprochera d'être daltonien. Quelle différence entre quelques cellules mal organisées du cerveau et quelques cellules mal venues de la rétine ? Cette fois c'est aux moralistes que nous posons la question.

Un problème de conception.

Les gouvernes des avions de transports modernes ne peuvent être actionnées directement par le pilote agissant sur le manche ou le palonnier. Les efforts aérodynamiques sur les gouvernes aux vitesses de croisières sont en effet trop importants pour pouvoir être équilibrés par une liaison mécanique entre commandes et gouvernes. Il est nécessaire d'assister le pilote en plaçant entre la commande et la gouverne un système amplificateur connu sous le nom de servocommande. Les servocommandes sont actuellement constituées par des vérins hydrauliques placés au voisinage des gouvernes. La commande des vérins est soit une commande mécanique (tringles et câbles liant le manche et le palonnier au tiroir de commande du vérin), soit une commande électrique (la position du manche est transmise par câble électrique à un moteur attaquant le tiroir du vérin, le plus souvent par l'intermédiaire d'un ordinateur).

Il est évident que la fiabilité du système de transmission des ordres du pilote aux gouvernes est fondamentale pour la sécurité du vol. Aussi les constructeurs ont-ils le souci permanent d'assurer une fiabilité optimale à ces systèmes.

Qu'entend-on par fiabilité optimale ?

Le premier réflexe consiste à proposer une absence totale de panne ! Hélas, tous les techniciens le confirmeront, la sécurité absolue n'existe pas, nous avons abondamment disserté sur ce sujet.

On peut améliorer la fiabilité d'un système en lui adjoignant des systèmes redondants, mais combien ?

Actuellement les systèmes de commandes hydrauliques sont triplés sur les avions de ligne et rendus physiquement indépendants (autrement dit la panne de l'un des systèmes est sans effet sur le bon fonctionnement des autres systèmes). Cette disposition conduit à une probabilité de perte totale des commandes de l'ordre de un sur un milliard par heure de vol (10^{-9}/h), la perte d'un seul système ayant une probabilité de l'ordre de un sur mille par heure (10^{-3}/h.) (voir le Chapitre 2 et l'Annexe 2).

Faut-il aller plus loin et installer quatre systèmes redondants ? Tous les techniciens interrogés répondront non à cette question pour plusieurs raisons,

- il n'est pas physiquement possible de disposer plus de trois vérins par gouverne sans avoir à effectuer des changements très délicats de conception,
- installer un système hydraulique supplémentaire augmentera la masse à vide de l'avion et réduira d'autant sa charge marchande (à masse au décollage constante imposée par des considérations de performances minimales assurant la sécurité au décollage),
- augmenter la complexité de l'installation du système hydraulique augmente les probabilités de non-indépendance des circuits redondants et ne va donc peut-être pas dans le sens de la sécurité (problème bien connu de la défiabilisation par un excès de souci de fiabilisation.),
- les autres systèmes vitaux de l'avion, circuits électriques, circuits d'alimentation en combustibles, structure, etc., ont des fiabilités voisines de celle du système hydraulique. Il serait illusoire d'augmenter la fiabilité du seul système hydraulique sans augmenter la fiabilité des autres systèmes, sinon la fiabilité globale de l'avion n'en serait pas augmentée pour autant.

On peut admettre que le premier argument est réfutable. Les ingénieurs n'ont qu'à faire preuve d'un peu d'imagination ! Il faut toutefois là encore penser au fait qu'augmenter la complexité ne va pas toujours dans le sens de la sécurité, comme le rappelle le troisième argument.

Au deuxième argument on peut répondre que le souci de la sécurité passe avant celui de la rentabilité. Ceci est vrai dans la mesure où les "améliorations" de sécurité ne rendent pas le produit fini économiquement inexploitable (rappelons le vieil adage, déjà cité, " la sécurité n'a pas de prix, mais elle a un coût! "), ce qui risque d'arriver si l'on augmente la fiabilité de tous les systèmes pour répondre au dernier argument. Quelle compagnie achèterait un avion de la taille de l'AIRBUS A380 pour transporter une vingtaine de passagers seulement parce que la place disponible dans le fuselage est pratiquement toute occupée par les systèmes !

En définitive l'ensemble des responsables de la conception des avions des générations actuelles est d'accord pour admettre que le triplement des systèmes hydrauliques est la solution raisonnable. On se reportera au chapitre 15 traitant du risque résiduel admissible.

Tout le monde admet donc qu'une probabilité de un sur un milliard par heure de vol pour la panne totale d'hydraulique est "raisonnable". Bien entendu, cela signifie que chaque concepteur s'assure que les systèmes

hydrauliques répondent aux règles de l'art et passent avec succès les épreuves sévères de qualification permettant d'affirmer que le niveau de un sur un milliard est raisonnablement assuré.

Il n'en reste pas moins qu'il reste une chance (ou plutôt une malchance) sur un milliard par heure de vol pour qu'une panne totale des circuits hydrauliques ne conduise un jour à la catastrophe.

Or ce n'est parce qu'un phénomène est hautement improbable qu'il ne se produit pas.

Envisageons une flotte de 4000 avions de la classe AIRBUS. Si l'on admet que chaque avion effectue en moyenne 14 heures de vol par jour (chiffre certainement sous estimé), cela représente 4000 x 14 x 365 # 20.000.000 heures par an. Ainsi la probabilité d'observer une panne totale d'hydraulique de probabilité élémentaire de 10^{-9}/heure, sur un avion de la flotte en 10 ans d'utilisation est-elle de l'ordre de vingt pour cent !

Que fera alors la justice si un tel événement malheureux se produit. ? Cherchera-t-elle un "coupable" ? Bien entendu il lui faudra s'assurer que toutes les règles de sécurité en matière de fabrication, maintenance, conditions d'emploi, formation du personnel ont été respectées et par le constructeur et par la compagnie utilisatrice.

Si une faute a été commise dans l'un de ces domaines, il lui faudra certainement condamner le coupable.

Mais il est parfaitement possible que l'accident ne provienne que de la conjonction malheureuse de la panne "normale et prévue" de chacun des trois circuits.

Et si à l'occasion de cet accident avec pertes de vies humaines, la justice venait à mettre son nez dans les dossiers d'incidents ? Cette fois ce sont les responsables de la sécurité qui se sentent mal à l'aise. Que répondre au juge d'instruction s'étonnant que des incidents analogues se soient déjà produits et que l'on n'ait pas encore réagi ? Plutôt que de risquer une mise en examen et une condamnation ne vaudrait-il pas mieux ignorer les incidents et mettre l'accident sur le compte de la fatalité.

Cette attitude peut sembler étonnante, mais nous avons connu des responsables d'une grande industrie refuser de faire des études de sécurité de peur de voir la justice se retourner contre eux dans le cas d'un accident survenant dans des conditions estimées hautement improbables au cours de l'étude et donc écartées à juste titre.

A l'occasion d'un accident aérien, nous avons vu en effet des magistrats, d'une nation étrangère et néanmoins amie, faire le raisonnement faux mais très convaincant suivant: "Vous me dites que cet événement est hautement improbable, soit, mais il s'est produit; par conséquent ou bien vous avez commis une faute d'estimation ou bien vous avez négligé volontairement de traiter ce cas; vous êtes donc coupable !".

Il est évident, pour tous les spécialistes des probabilités que "hautement improbable" ne signifie pas impossible. Pour s'en convaincre il suffit de calculer la probabilité de gagner le gros lot au Loto, c'est-à-dire de prévoir six numéros gagnants sur quarante-neuf. Il y a environ une chance sur quatorze millions de gagner, événement par conséquent hautement improbable. Or presque à chaque tirage il y a un gagnant, ce qui ne signifie pas que le calcul de la probabilité soit faux, mais que le nombre de joueurs est grand! En effet la probabilité pour qu'il y ait un gagnant si vingt millions de grilles ont été joués est de 76 %. Elle monte même à 98,6 % pour trois tirages de vingt millions de grilles. Les curieux trouveront en annexe 2 la justification de ces chiffres.

Une fois de plus ce n'est pas au technicien de trancher. Nous nous contenterons de poser le problème qui est loin d'être un cas d'école fabriqué pour la cause.

Il nous parait intéressant de citer, à cette occasion, Monsieur Raymond Nivet, Ingénieur des Arts et Manufactures, Expert agréé par la Cour de Cassation. Dans un article publié en Octobre 1989 dans la revue EXPERTS, il écrit:

"Incidemment, la montée en puissance du consumérisme s'est naturellement traduite par une augmentation considérable des actions intentées contre les constructeurs. Cette tendance a malheureusement un effet néfaste sur la sécurité aérienne; on peut comprendre une tendance chez les constructeurs à limiter la circulation des informations sur les incidents ou dysfonctionnements, ou ce qui revient pratiquement au même, à les faire transiter par leurs services juridiques. Pire encore, ils pourront hésiter à imposer les modifications au matériel que l'étude d'un incident feraient apparaître souhaitables sinon nécessaires, de peur que cette démarche soit interprétée comme un aveu de négligence ou imprudence dans la mise en service de ce matériel dans sa configuration initiale."

Cet état d'esprit, fâcheux, mais bien compréhensible, ne se rencontre pas que dans le domaine aéronautique. Citons quelques exemples dans le domaine médical.

Le cancer du larynx peut être soigné de deux façons,

- par voie chirurgicale (laryngectomie partielle conservatrice) qui risque de provoquer des pneumopathies ou des accidents post opératoires (risques faibles mais non nuls) mais qui conduit à la guérison du cancer dans 90% des cas,
- par radiothérapie ce qui ne conduit à la guérison que dans 60% des cas.

Actuellement la première solution n'est pas pratiquée aux États Unis car un échec est mis sur le compte du chirurgien, alors que pour la seconde méthode un échec est mis sur le compte de la maladie. Or il est évident que statistiquement, un malade a intérêt à suivre la première méthode car le risque est faible et l'espérance de gain importante pour lui, alors que le chirurgien a intérêt à suivre la seconde car il finira bien, un jour ou l'autre, s'il suit la première, par tomber sur un mauvais cas qui lui sera préjudiciable.

Un certain nombre de fractures relève de traitements chirurgicaux permettant de "réparer" le squelette endommagé à l'aide de prothèses internes provisoires ou définitives. Or ces techniques ne sont pas utilisées aux États Unis. On leur préfère des fixateurs externes qui réparent moins bien, mais qui ne font courir aucun risque au médecin qui ne peut se voir reprocher un accident, rare là encore mais possible, lié à l'acte chirurgical, en particulier à l'anesthésie, ou au risque d'infection.

Enfin, et nous nous en tiendrons là pour éviter la lassitude chez le lecteur, le nombre d'accouchements par césarienne augmente régulièrement aux États-Unis, non parce que les femmes deviennent plus fragiles, mais parce que le risque de procès est plus faible pour le gynécologue que lorsque l'accouchement est pratiqué par voie naturelle.

Il se trouve qu'heureusement les ravages du consumérisme ne se sont pas encore trop fait sentir en France, mais nous sentons venir l'orage. L'affaire récente de la non détection par échographie d'une malformation du fœtus in utero doit nous mettre en garde contre la tentation de supposer que tout dysfonctionnement ne peut que provenir de la faute du praticien. De toute façon nous voyons difficilement, dans le climat actuel, un chirurgien ou un médecin faire part à ses confrères de sa dernière erreur pour les mettre en garde et leur faire profiter de son expérience, malheureuse, mais instructive. Cependant, comme le montrent de nombreux articles de la revue "Responsabilité" (revue de formation sur le risque médical dont le numéro 1 date de mars 2001 et dont le président du conseil de rédaction est le Professeur Claude Sureau, ancien président de l'Académie de Médecine), le corps médical a pris conscience de la nécessité du Retour d'Expérience et œuvre dans ce sens.

En conclusion nous pensons que l'application rigoureuse du Code pénal en matière d'accident du travail peut conduire à une amélioration de la sécurité en montrant aux dirigeants que le non-respect des règles de sécurité n'est peut-être pas rentable. Elle risque toutefois d'avoir un effet pervers en poussant ces mêmes dirigeants peu scrupuleux à faire de la "sécurité juridique", c'est-à-dire se contenter d'appliquer la lettre des règles de sécurité sans se soucier de leur efficacité.

Par contre l'application trop rigoureuse de la loi, dans les cas complexes du type de ceux que nous avons évoqués, en cherchant à tout prix un coupable, est néfaste à la sécurité en ce sens qu'elle conduit tous les acteurs industriels à se garder de faire part de leurs erreurs à la communauté de peur de voir leur franchise se retourner un jour contre eux à l'occasion d'une catastrophe.

Or l'amélioration de la sécurité passe impérativement par le retour d'expérience, c'est-à-dire par la connaissance des erreurs et défaillances rencontrées en service n'ayant pas entraîné de catastrophe. Les accidents sont trop rares, heureusement, pour que l'on se contente de leurs analyses pour en tirer des leçons. Par contre les incidents sont multiples et porteurs de toute l'information nécessaire à la compréhension et à la prévision des chaînes d'événements conduisant à la catastrophe. Encore faut-il pouvoir les connaître. Seul un climat de confiance, déculpabilisant, permettra de recueillir ces informations fondamentales.

Messieurs les juristes, s'il vous plaît, aidez-nous dans cette démarche !

Il nous faut mettre en évidence un autre obstacle d'origine juridique au Retour d'Expérience.

A l'occasion d'un accident, la justice a pour rôle de déterminer les responsabilités et a donc pour souci majeur, que nous ne lui contestons pas, de préserver les preuves. Cela se traduit par une protection physique de la situation résultant de la succession des événements ayant conduit à la catastrophe. Cette protection, nécessaire pour éviter une falsification possible des preuves, se traduit par deux types d'actions.

La mise sous scellés des divers enregistrements, bandes magnétiques, disquettes, disques durs, photographies, films etc..

La mise sous scellés des preuves matérielles, en particulier épaves, pièces cassées, locaux incendiés, produits chimiques plus ou moins dégradés, etc.

On comprendra la frustration des ingénieurs responsables de la sécurité qui pensent que l'explication de la catastrophe ou du moins les circonstances précises ayant précédé la catastrophe, se trouvent dans les enregistrements qu'ils ne peuvent consulter. On comprendra leur anxiété à l'idée qu'un autre accident est possible et qu'ils ne peuvent le prévenir faute d'éléments leur permettant de trouver un remède.

On comprendra également leur regret de voir des informations disparaître du fait de la mise sous scellés des preuves matérielles. En effet l'analyse d'une fracture fraîche sur une pièce peut fournir des informations sur les causes de cette rupture, fatigue, dépassement de la limite d'effort statique ou d'effort dynamique, etc. La corrosion de la fracture par oxydation à l'air masque peu à peu ces informations avec le temps. Il en va de même des produits chimiques résultant par exemple d'une combustion. Les réactions chimiques se poursuivent inexorablement et il est de plus en plus difficile de remonter aux informations initiales.

On objecte bien souvent que pour assurer la sécurité en attendant la levée des scellés, il suffit d'arrêter l'exploitation du système en cause. Mais les conséquences économiques d'une telle mesure peuvent être catastrophiques. Il est évident que si la sécurité est en cause, il est plus que raisonnable d'interdire de vol tel type d'avion. Est-ce justifié par de simples considérations juridiques ?

Pour pousser les choses au pire que se passerait-il si un accident se produisait suite à une protection malencontreuse des preuves, par exemple explosion de produits chimiques mis sous scellés ? Le juge d'instruction serait-il considéré comme l'un des responsables de ce nouvel accident ?

Il nous parait indispensable de concilier les objectifs des techniciens et des magistrats. En aucun cas les techniciens ne désirent entraver le cours de la justice et nous ne pensons pas que les magistrats n'aient pas le souci d'assurer la sécurité. Il est donc fondamental de dégager des procédures de préservation des preuves sans pour autant en empêcher la consultation par des personnes compétentes. Il ne nous parait pas impossible de réaliser des copies conformes des enregistrements sans détérioration des originaux et avec toutes les garanties juridiques de leur non-falsification. Il ne nous parait pas impossible de pratiquer l'analyse des pièces en présence d'experts et de magistrats garants de la non-destruction des preuves.

Il est évident que la mise au point de ces procédures doit se faire en dehors de toute situation de catastrophe. En conclusion de ce chapitre, nous proposons donc la mise sur pied de groupes de travail juristes - techniciens pour bâtir ces procédures dans les principaux domaines de la technique, nucléaire, chimie, pétrole, transports terrestres, maritimes, aériens, etc. La sécurité a tout à y gagner et la justice n'a rien à y perdre.

Ce chapitre constitue une mise à jour d'un article paru dans la revue "Préventique" n° 46 Juillet/Août 1992. La première partie a été présentée au colloque "Juriste Ingénieur" de Mars 1993 organisé par l'École Nationale de la Magistrature et l'Institut Européen de Cindynique.

CHAPITRE 15

Le météore qui avait détruit le réservoir d'oxygène du vaisseau spatial "Star Queen" était un géant, d'au moins un centimètre de diamètre et pesant au moins dix grammes. En se référant aux tables, le temps moyen entre deux collisions avec un tel monstre, était de l'ordre de dix puissance neuf jours, soit trois millions d'années. La certitude virtuelle qu'un tel événement ne se reproduirait pas au cours de l'histoire de l'humanité ne donnait qu'une faible consolation à l'équipage.

Extrait de la nouvelle de science fiction "Breaking Strain, expedition to Earth"
de Arthur Clarke, membre de la Royal Astronomical Society.

LA NOTION DE RISQUE ADMISSIBLE

Y a-t-il un risque admissible ? Cette question a-t-elle même un sens ?

De quel genre de risque s'agit-il ? On ne considérera ici que les risques touchant la vie ou la santé des hommes et on écartera les risques de nature économique, financière, industrielle etc. C'est bien d'ailleurs lorsqu'il y a victime que l'opinion publique s'émeut, demande des sanctions contre les coupables et clame "plus jamais cela". Pour des raisons affectives et psychologiques notamment, cette attitude se comprend parfaitement et nous sommes tous susceptibles de l'avoir un jour ou l'autre. Autant un individu est prêt à admettre, non sans douleur, un deuil résultat d'un cataclysme naturel incontrôlable et imprévisible, autant il admet fort mal qu'il soit plus ou moins le fait d'une erreur ou négligence humaine et que, par conséquent, il aurait pu être évité. En raison des progrès de la médecine, même le décès suite à maladie n'est plus systématiquement admis, si l'on a l'impression que le malade aurait pu être mieux soigné.
On n'abordera pas ici ce problème des responsabilités ou culpabilités, civiles ou pénales et on se limitera à une analyse des risques et à cette notion très floue, pour l'opinion comme pour les acteurs concernés, de risque admissible. Mais un risque peut-il être admissible, tolérable ?
On dira sans doute qu'il peut en être ainsi si l'on est le seul concerné ou si l'on appartient à un groupe spécifique qui l'accepte délibérément. Après tout, un alpiniste prend des risques et le sait. Mais si d'autres que les "volontaires" subissent les effets des risques pris, qu'en est-il alors ?
On verra que cette notion incertaine, et même ambiguë, de risque admissible est cependant inévitable.

Risques et activité humaine

Nous reprenons ici quelques notions qui ont été développées dans le chapitre 2 afin de mieux cerner le problème du risque admissible sans se référer à ce lointain chapitre.

Toute activité humaine implique un risque. C'est vrai des activités les plus triviales telles que la promenade en famille, et cet exemple montre que les parents acceptent alors un risque pour leurs enfants. Ne parlons pas du bricolage ou jardinage du dimanche, souvent dangereux. Phénomène bien connu des hôpitaux! Ces risques-là sont généralement acceptés par habitude : ils sont "à taille humaine". C'est le cas du coup de marteau sur le doigt où l'on ne peut invoquer que sa propre maladresse; mais que dire de la scie électrique ou de la tondeuse à gazon mal protégée ou dont on a ôté la sécurité ?
Mais l'activité humaine génère des risques plus complexes et souvent collectivement plus importants dès lors que des énergies importantes sont mises en jeu. Citons les moyens de transport (automobile, chemins de fer, bateaux, avions), les bâtiments (feu, ascenseurs, conduites de gaz...), les grandes installations industrielles (chimie, énergie, nucléaire...) et même les gradins d'un stade de football ou les boites de nuit. Bien entendu, les acteurs s'appliquent très généralement à "*prendre des précautions*" et s'efforcent de minimiser les risques courus. C'est surtout vrai dans les grands projets industriels où la minimisation des risques fait partie des "règles du jeu".
Dans des domaines moins ambitieux techniquement, la prévention du risque se limite souvent à un respect des règlements : issues de secours de la boite de nuit, non inflammabilité des matériaux etc. On suppose alors que la puissance publique ou ses agents "ont fait leur métier" et que le respect du règlement assure la sécurité, quitte à tout remettre en cause si, malheureusement, un accident se produit.

Dans l'industrie jusqu'aux environs des années 60, l'idée était confusément répandue que le risque nul existait. Cette idée est encore d'ailleurs très présente dans l'opinion, la publicité et surtout les médias. "*Nous avons fait tout le nécessaire, vous ne risquez rien". "Un tel accident ne se produira jamais plus".* Ou, plus chauvin : "*Un tel événement ne peut pas se produire en France*". Bien sûr, des accidents se produisaient quand même; ils étaient alors nécessairement le résultat de négligences, de légèreté, voire de méchanceté ou, *in fine,* à défaut, de la fatalité. Le destin, bref ! Des ratés du système, mais il fallait poursuivre l'objectif du risque nul.
Des exemples ? Des marges de calcul importantes assurent que le pont résistera à des charrois bien plus lourds que la charge maximale autorisée (ce qui permit pendant la guerre à des chars de 10t de franchir des ponts limités à 1,5t!) ou que le téléphérique peut supporter 5 fois la charge maximale de skieurs. Des procédures bien définies assurent la sécurité dans des situations opérationnelles ou de pannes bien définies. Il suffit alors de les respecter. C'est ce que certains appelaient la *sécurité intrinsèque*.
L'approche précédente rassure, mais elle est un mirage, un mirage dangereux. C'est la *méthode de l'autruche* : le danger n'existe plus. Puisqu'il n'existe plus, point n'est besoin de l'identifier. C'est le tout ou rien. A défaut d'inventaire, des éléments sont restés inaperçus dans un tiroir, ou bien se sont introduits subrepticement après inspection du dit tiroir.
Le pont est surabondant, mais par fort vent, peut apparaître un phénomène vibratoire, dit de flottement, qui le détruit rapidement (pont de Tacoma aux États-Unis). Le téléphérique est surabondant statiquement, mais l'on a changé de matériau pour la potence et des phénomènes de fatigue, inconnus ou négligés auparavant à juste titre, deviennent déterminants (accident d'un téléphérique dans les Alpes françaises au début des années 60). Les procédures définies sont correctes, mais apparaissent des circonstances ou des pannes non envisagées, un malentendu, une rédaction ambiguë et la porte du ferry n'est pas fermée ou le frein du train n'a plus de pression ou deux trains sont envoyés en sens inverse sur une voie unique sans possibilité de les intercepter et de les stopper.

Puisqu'il est inévitable qu'un risque résiduel existe, mieux vaut essayer de l'identifier, de le chasser avec obstination, ou à défaut de le borner. Comme, de plus, le travail effectué est imparfait et que les circonstances peuvent changer, il faut que cette activité soit continue, aidée d'une surveillance non moins continue.
Une évolution importante s'est donc développée il y a quelques quarante ans. L'apparition de systèmes très complexes (comme peuvent l'être un avion moderne, une aventure spatiale, une centrale nucléaire), l'importance des dangers courus (avions de plus de 400 places, risques liés aux matières fissiles...), l'usage de technologies ou l'exploration de domaines d'action sur lesquels l'expérience est faible (Concorde, espace, centrales nucléaires...) rendaient indispensable ce changement de méthodologie.
On a donc entrepris des analyses très détaillées des risques éventuels avec des arbres de défauts possibles, une analyse des conséquences etc. Un tel travail étant quasiment infini si l'on ne le borne pas, on a tenté de quantifier les probabilités des événements élémentaires participant à cette analyse. Si une probabilité trop basse peut être attribuée avec confiance à un événement ou combinaison d'événements, la situation correspondante peut alors être négligée. Bien entendu, les résultats d'un tel travail sont constamment utilisés pour concevoir et justifier un système aussi sûr que possible.
De plus, pour éviter les risques liés à des estimations erronées de bonne foi, une surveillance continue en exploitation permet de justifier qu'il n'y a pas d'erreur grossière sur les probabilités estimées ou, dans le cas contraire, de revoir l'analyse, les procédures et même la conception.
La description des méthodes permettant de mettre en œuvre le rouleau compresseur évoqué ci-dessus sort du cadre de cet ouvrage. Disons simplement que leur application apporte beaucoup au concepteur comme à l'exploitant et que leur application à des installations ou systèmes conçus antérieurement auraient été féconde.

On conçoit bien les principaux **avantages** d'une telle approche :

- Elle oblige tous les concepteurs, pour définir, justifier tant les matériels que les procédures, à un constant souci de sécurité. Elle implique tous les acteurs et leur fournit une méthode de travail unique dans un projet donné.
- Elle fournit un guide âne pour reconnaître ce qui est acceptable et ce qui ne l'est pas. Ceci n'évacue nullement l'expérience et le bon sens, mais leur ajoute un juge de paix supplémentaire.
- Elle permet d'estimer l'opportunité ou l'inopportunité de tel dispositif ou de telle modification. On s'apercevra, par exemple, qu'une disposition qui paraissait bénéfique au premier coup d'œil, mais qui complique le dispositif, n'apporte éventuellement rien par suite d'effets seconds.
- Elle requiert généralement la constitution d'un service ou bureau Sécurité qui définit les méthodologies à appliquer, revoit les analyses et les synthétise, décloisonnant ainsi les spécialistes de diverses disciplines.
- Elle identifie les points difficiles et potentiellement critiques qui devront faire l'objet d'une surveillance particulière pendant les essais et en utilisation.
- Elle identifie le niveau de sécurité visé, que l'on espère atteint et, *a contrario*, les événements, circonstances ou pannes que l'on a délibérément acceptés de ne pas considérer.

A l'évidence, cette approche est à la fois plus réaliste et plus sûre que celle de l'autruche. Elle n'est pas non plus sans danger et recèle un certain nombre de **pièges** si elle est appliquée sans discernement. Sans entrer dans trop de détails, prenons quelques exemples.

- L'estimation des probabilités élémentaires de situations ou de pannes n'est pas toujours de la même qualité. Il existe une probabilité de se tromper sur la probabilité! La probabilité de rafales d'une certaine importance est connue avec une assez grande précision. Mais tous les phénomènes ne sont pas aussi bien connus. La panne simple aux effets catastrophiques doit donc être systématiquement écartée, sauf justification "en béton", en raison des conséquences considérables que peut avoir une erreur d'estimation.
- La combinaison des probabilités pour estimer le résultat pour une situation complexe ressort de méthodes logiques et mathématiques bien maîtrisées. Mais il peut exister des risques cachés résultant d'interactions non évidentes et passant par des chemins très détournés. Par exemple, plusieurs circuits hydrauliques, indépendants et correctement ségrégués, peuvent se trouver vibrer sur une même fréquence mécanique, générée rarement, mais occasionnellement par tel équipement, et, en conséquence tomber en panne de manière quasi-simultanée.
- Il est important que les situations potentiellement catastrophiques résiduelles soient grossièrement équiprobables. Dans le cas contraire, une erreur d'estimation pourrait avoir des conséquences démesurées par rapport à l'erreur commise. Ce point a déjà été cité au chapitre 2, rappelons en l'explication. Supposons que le taux de risque accepté corresponde à une probabilité de catastrophe inférieure à 10^{-7} par heure de fonctionnement et que ce risque résiduel résulte de 100 situations catastrophiques ayant chacune une probabilité de $10^{-9.}$ Une erreur d'un facteur 100 sur l'une de ces situations lui donnera une probabilité de 10^{-7}, et la probabilité globale de catastrophe passera à 2.10^{-7}, dégradation encore tolérable. Si, en revanche, la probabilité globale de catastrophe résulte d'une situation ayant une probabilité de $0,9.10^{-7}$ et de 99 autres se partageant le $0,1.10^{-7}$ restant, une erreur d'un facteur 100 sur la première situation lui conférera une probabilité de $0,9.10^{-5}$, totalement inacceptable.
- Il y a des risques externes spécifiques qui n'apparaissent pas naturellement dans une étude de sécurité. Faut-il considérer le crash d'un B747 sur une centrale nucléaire. Et l'arrivée d'un météorite ? De quelle taille ? Comment assurer qu'un logiciel vital est libre d'erreurs. Sauf précautions particulières, une même erreur peut affecter tous les éléments supposés indépendants et redondants.
- Les opérateurs peuvent commettre des erreurs. Les systèmes doivent le prévoir et faire en sorte que les conséquences n'en soient pas catastrophiques. Mais doit-on supposer que le pilote d'un avion de transport va délibérément passer sous le téléphérique de l'aiguille du Midi, pour faire joli ?etc.

Même appliquée correctement, avec soin et discernement, la méthode suivie n'est pas sans poser un certain nombre de problèmes à l'opinion publique, au monde juridique, aux assurances etc. Car, d'une certaine manière, elle montre clairement que l'accident est "non-improbable", que, d'une certaine manière, il était "prévisible". Le technicien dira, non sans raison, que l'application de la méthode ne crée pas le risque - elle conduit même à mieux le réduire. Le risque existait même auparavant, au temps de la sécurité intrinsèque. Simplement, on ne l'identifiait pas, on ne le quantifiait pas aussi clairement : il n'apparaissait pas dans les dossiers de justification ! Qu'en résulte-t-il en cas d'accident ?

Nous prendrons trois exemples tous empruntés au monde aéronautique.

- La distribution des rafales dans l'atmosphère est bien connue avec une assez bonne précision en raison de nombreuses études conduites dans le monde entier depuis longtemps. Les avions sont calculés pour résister sans dommages sérieux à un certain niveau de rafales dont la probabilité est bien déterminée. De plus, il existe des statistiques tenues à jour par l'expérience en service et les méthodes de calcul et de justification des structures sont bien maîtrisées avec une grosse expérience.

  Un jour, au-dessus de la Sierra Nevada américaine, un B52 de l'US Air Force rencontra la rafale du siècle et la dérive cassa. Par chance, l'équipage réussit à ramener l'avion au sol, mais l'accident n'était pas passé loin. La même aventure aurait aussi bien pu survenir à un avion civil.
- Pour la plupart des avions de transport actuels, l'existence d'énergie hydraulique est vitale : la vitesse et la taille des avions rendent impossible l'usage de la seule force humaine pour déplacer les gouvernes. La pérennité de la fourniture hydraulique est généralement assurée par trois circuits indépendants, dûment ségrégués, et dont les équipements constitutifs sont très fiables et, de plus, fortement redondants. Nous avons déjà cité cet exemple au chapitre 12.

  Sur un DC10 américain, une avarie du réacteur central, pourtant envisagée, conduisit à une projection de débris à haute énergie suivant une distribution spatiale fort peu probable : les trois circuits furent coupés. L'équipage, qui n'avait plus de commandes de vol du tout, réussit le tour de force, à l'aide d'un

pilotage différentiel des deux moteurs restant et grâce à la collaboration du Contrôle au sol, à ramener l'avion vers un terrain de secours où l'avion fit néanmoins un crash assez violent : il y eut des morts mais aussi des survivants, revenant de très loin. En un sens, cet accident était prévisible.

- Les avions sont conçus pour résister au givrage, qui est un phénomène assez bien connu et bien quantifié. Les règlements fixent les givrages maximaux à considérer, ce qui veut dire que des givrages plus sévères sont possibles et sont quelquefois, très rarement, rencontrés.

Qu'est-ce alors qu'un risque admissible ?

Y a-t-il donc un risque admissible ?
Une première réponse consisterait à dire : **c'est le risque contre lequel je ne peux rien**. La fatalité en quelque sorte. Nous ne pouvons en rien nous prémunir contre un météorite qui nous tomberait sur la tête ; nous sommes donc obligés d'admettre ce risque.
En fait, même cette réponse élémentaire est plus complexe qu'il n'y paraît. Nous pourrions nous promener munis de casques-parapluie résistant à certaines tailles de météorites, qu'imaginerait sans peine ce cher savant Cosinus. Laissons la facétie de côté pour constater que l'impuissance varie avec le temps et les progrès de la technique. Pour l'instant, on ne sait guère annoncer les tremblements de terre. Il y a pourtant des pays à risques. Faut-il évacuer le Japon, la zone de San Francisco et la région de Nice ? Et pourtant, sur longue période, un tremblement de terre y est probable! Les risques volcaniques sont moins imprévisibles ; prend-on pour autant toutes les mesures nécessaires pour qu'une éruption ne cause pas de victimes ?

Mauvaise réponse à notre question.

Le risque admissible est-il celui que **l'opinion publique** tolère ? En un sens certes, car, d'une manière ou d'une autre, l'opinion publique aura toujours finalement raison. Mais ce risque ainsi défini est-il en fait défini, contrôlable, maîtrisable **?**

L'opinion publique se montre souvent incohérente, comme d'ailleurs chacun des membres qui la constitue, car il est bien établi que le danger ou le risque est une notion que les humains apprécient naturellement fort mal. Telle personne refusera de prendre l'avion parce que c'est trop dangereux, mais n'hésitera nullement à prendre sa voiture, beaucoup plus dangereuse, ou à faire de la varappe.

Est-ce l'impression confuse de la maîtrise de soi ? **Je** conduis ma voiture moi-même et **je** fais de la varappe. Bref, je suis maître de moi comme de l'univers, mais peu disposé à me livrer à d'autres. Comportement psychologiquement explicable, mais erroné. Le risque aérien tient compte des populations de pilotes telles qu'elles sont. Et en voiture, je cours des risques du fait des autres. Je suis loin d'être infaillible moi-même et n'ai point besoin d'être extralucide pour m'en apercevoir.
Incohérente, l'opinion publique l'est aussi suivant les secteurs de l'activité humaine. Un accident circonscrit à l'intérieur d'une centrale nucléaire et qui ferait 10 morts, soulèverait beaucoup plus d'indignation que la mort de 30 personnes dans un carambolage général sur autoroute. Les accidents provoqués par le gaz dans nombre de villes sont moins dramatiquement perçus qu'un accident d'avion, quoique ceux-ci commencent à se banaliser dans l'opinion.
L'incohérence peut aussi se manifester dans les échelles de temps. Un crash unique faisant 500 morts en une fois et survenant une fois dans l'année est beaucoup plus mal ressenti que 10 crash à 50 victimes chacun étalés sur un an. Quant aux accidents de la route, ils semblent faire partie de l'inévitable, à telle enseigne que l'opinion publique s'élève quelquefois contre des mesures destinées à améliorer la sécurité routière. Que dire par exemple des événements statistiquement non significatifs avancés pour récuser le port de la ceinture ou du report du projet de loi relatif aux grands excès de vitesse ?
C'est pour des raisons quantitatives de ce genre que la FAA américaine (Federal Aeronautical Agency) décida pendant les années 60 de revoir les règlements applicables aux gros porteurs, B747 d'abord puis DC10, Lockheed 1011, Airbus A300, pensant qu'un crash faisant plus de 300 morts ferait réagir plus fortement que des crashs faisant environ 100 morts. La FAA a eu raison d'ailleurs, même pour de mauvais motifs, car, la technique le permettant et l'application des nouveaux règlements ayant été généralisée, il en est résulta une amélioration notable de la sécurité. Nous renvoyons volontiers aux propos déjà cités de Jean Anouilh dans *l'Hurluberlu*, se demandant ce qui est le plus triste : une veuve ou 100 veuves ? 100 veuves est-il 100 fois plus triste qu'une veuve ? Allez donc le demander aux intéressées !
Enfin, l'opinion publique n'est pas exempte de passions, par nature irrationnelles.

Récusons donc également l'opinion publique.

Le risque admissible se définit-il alors par la négative, à savoir, celui **qui n'est pas prohibé**. C'est alors le législateur qui est juge et le droit qui codifie. Nous faisions plus haut allusion à la sécurité conçue comme respect du règlement, en parlant des issues de secours et de l'ininflammabilité des matériaux dans une boite de nuit. C'est une solution bien commode pour l'industriel concepteur comme pour l'exploitant. Leurs tâches et leurs devoirs sont clairs. C'est également commode pour les assurances et en cas de litige. "*Le règlement c'est le règlement*" : le gendarme sait comment s'y prendre.
Mais en fait, il faut se demander pour quel motif et comment le législateur a légiféré ?
Il a pu agir en toute bonne foi et dans un réel souci de sécurité. Mais son action résulte d'avis d'experts et des connaissances à une époque donnée. Les phares jaunes ont été introduits en France pour des raisons de sécurité. Leur obligation a été supprimée récemment subrepticement pour des raisons d'harmonisation européenne, sans doute. A-t-on justifié l'erreur éventuelle associée à la première mesure, à savoir que les phares jaunes n'amélioreraient pas la sécurité, ou l'importance accordée à la seconde, si elle réduit effectivement la sécurité ? Rappelons qu'à la suite de la catastrophe de Tchernobyl un certain nombre d'états européens ont décrété qu'il était interdit de commercialiser des produits alimentaires dont la radioactivité ne serait pas strictement nulle en oubliant totalement la radioactivité naturelle ! Respecter la réglementation aurait conduit à périr de faim devant des monceaux de victuailles réglementairement impropres à la consommation.
Le règlement renvoie aux experts et, par conséquent à l'état de l'art et de la technique.
Mais la question est souvent plus compliquée encore. Le législateur est soumis à de nombreuses pressions, celles de ses opposants politiques, celles de son électorat, celles de l'opinion publique, celles des professions, des lobbies, ces dernières étant officielles et quasi codifiées aux États-Unis et plus souterraines en France.

Récusons-nous aussi le législateur ?

Le risque admissible est-il une question sans réponse ?

Sûrement pas sans réponse, car ne pas répondre constitue une réponse : le hasard, à moins de suspendre toute activité humaine, ce qui est dépourvu de sens.

Cependant, il n'existe pas de bonne réponse totalement inattaquable. Parlons donc de ce qui constitue, semble-t-il, la moins mauvaise solution.

Elle consiste à inventorier le plus sérieusement possible les risques courus, à les quantifier, à essayer de définir un niveau jugé tolérable, et par conséquent admissible, à une époque donnée, dans des circonstances données, sur la base d'un consensus national, ou mieux international si c'est possible, consensus explicite ou implicite.
Par consensus explicite, nous entendons celui qui résulte des actes d'une conférence ou d'un organisme qui enregistre le niveau de sécurité requis et, pour être réaliste, les moyens acceptables de le justifier. Le consensus est implicite s'il est obtenu par référence à un état de l'art et à des statistiques opérationnelles qui identifient en fait le niveau requis.
Ne reprenons pas le Discours sur les méthodes, à peine esquissé plus haut, et tentons d'identifier les failles et les mérites de cette "moins mauvaise réponse".

Le consensus auquel nous nous référons est nécessairement un consensus d'experts. Ceci ne veut pas dire qu'il ne tienne pas compte de l'opinion publique, de la volonté politique etc.. Mais seuls des experts peuvent identifier ce qui est possible et ce qui ne l'est pas, manipuler les concepts pertinents pour une technologie donnée, identifier la nature des risques courus et traduire le tout sous une forme intelligible, non ambiguë, scientifiquement correcte etc.

Le recours aux experts est une faiblesse, mais comment faire autrement ? Expert ne veut pas dire infaillible, ni extralucide. De plus, les experts sont inévitablement influençables et influencés. Ils appartiennent par nature à un certain milieu technique ou scientifique; ils en partagent les qualités et les défauts. Ils sont inévitablement déformés par ce qu'ils sont.
De plus, ils sont soumis à des pressions, volontaires ou non, coupables ou innocentes. Leur milieu professionnel d'abord. Experts du nucléaire par exemple, c'est un secteur d'activité qui les intéresse, les passionne. Il n'y a jamais très loin entre l'information nécessaire en provenance du milieu professionnel et la pression d'intérêts techniques, sociaux, financiers.
Qu'ils soient experts officiels, d'État ou délégués à ce titre, ou experts privés, ils peuvent être l'objet de pressions politiques, économiques ou financières. Sournoises, elles peuvent être les plus pernicieuses; telle attitude va être défavorable à l'industrie française qui a investi ailleurs, entraîner du chômage, entamer la balance du commerce

extérieur; réfléchissez bien aux conséquences de vos décisions d'experts, ne restez pas drapés dans une position de vestale etc.
L'opinion publique peut jouer un rôle pervers. Une décision technique qui serait parfaitement fondée et faciliterait de fait l'extension des centrales nucléaires serait mal venue. Sans prendre parti sur le fond, il suffit de voir le niveau des arguments pour ou contre Super-Phénix pour réaliser que la sérénité technique ne coule pas de source.
Le rôle éventuel de la justice peut aussi avoir des effets pervers. La perspective d'avoir peut-être un jour à témoigner ou à se défendre dans une action en justice peut distordre le jugement technique et conduire à prendre les décisions les plus faciles à défendre en justice et non les plus appropriées pour la sécurité. C'est le cas actuellement aux États-Unis dans le domaine médical. Devons-nous rappeler qu'il fut une époque où, étant partie dans un accident de la circulation, porter secours à une victime était quelquefois interprété comme un aveu de culpabilité!

Malgré tous ces défauts, cette approche du problème est quand même la moins mauvaise possible, pour toute une série de raisons qui ont été explicitées plus haut. Paraphrasant W.Churchill, on pourrait dire que c'est la plus mauvaise des méthodes, mais que les autres sont encore pires.
La lucidité implique cependant d'essayer de minimiser les défauts du système. Outre des principes d'ordre éthique de la profession et une application rigoureuse de méthodes bien identifiées, la meilleure parade est à trouver dans un caractère suffisamment international de la réglementation, y compris les méthodes de conformité, et des instances de contrôle. En effet, il est extrêmement rare que les intérêts des divers pays, des divers constructeurs coïncident et que les pressions politiques et autres s'additionnent sans heurts. Ceci réduit les risques de dérapage et, au pire, les homogénéise.
Cependant, le jour où le libéralisme et la déréglementation sans contraintes et le jeu de la concurrence débridée auront conduit, dans le domaine du transport aérien, à un constructeur aéronautique unique, à un exploitant unique, à une autorité unique de navigabilité et à une cour de justice internationale unique installée à Panama ou à la république de Saint Marin, il y aura lieu de s'inquiéter de la sécurité dans ce domaine. Nous n'en sommes pas encore là. Croisons les doigts.

Signalons un autre effet pervers potentiel de l'utilisation des avis d'experts. Dans un domaine d'activité donné, les experts préconisent un niveau de sécurité acceptable compte tenu des solutions technologiques disponibles à un moment donné. Au cours du temps les possibilités de la technique et les contraintes économiques évoluant, il est possible de resserrer les exigences. "On peut faire mieux, pourquoi ne pas demander plus ?" sera tenté de déclarer l'expert. Le problème est de savoir jusqu'où il est raisonnable d'aller.

Reprenons un exemple déjà cité.
Il est raisonnable de limiter le rejet de polluants en provenance d'une industrie de fabrication de produits chimiques. A un moment donné il est possible, avec des moyens techniques acceptables sur le plan économique, de limiter le taux de pollution à proximité des unités de production à une valeur de x%. Ce taux n'est pas fameux, mais moyennant quelques précautions vis à vis de la population voisine, les risques encourus, disent les experts, sont raisonnablement faibles. Les améliorations de la technique aidant, on voit apparaître une possibilité de réduire le taux de pollution. La décision, dans ce cas, ne fait aucun doute. Il faut renforcer les exigences et imposer ces nouvelles solutions technologiques. Arrive un moment où le taux de pollution, de l'avis d'une communauté d'experts, ne présente plus qu'un risque dit acceptable pour les populations du voisinage. Tout le monde est satisfait, bien que la querelle sur l'effet des faibles doses opposent et opposeront toujours les scientifiques et les écologistes purs et durs.
Puis les améliorations technologiques se poursuivant, il devient possible de diviser encore par un facteur cent le taux de pollution. Certains experts déclareront "Qui peut le plus, peut le moins. Puisque cela est possible, sur le plan technique et sur le plan économique, pourquoi ne pas l'exiger ?".
Est-ce bien raisonnable ? La réponse n'est pas évidente.
Cette amélioration technologique ne recèle-t-elle pas des vices cachés qui peuvent créer des risques différents et nouveaux ?
Rappelons l'exemple fabriqué pour la circonstance, mais réaliste. Nous pouvons réduire la quantité de polluants rejetés en balayant les unités de production avec un gaz inerte, de l'azote par exemple. Dans ce cas ne risquons-nous pas d'augmenter le risque d'asphyxie des travailleurs pour réduire, inutilement, un risque négligeable dans les populations voisines ?
Par ailleurs toute modification a un coût, économiquement acceptable peut-être, mais qui demande quand même un financement. Ne serait-il pas plus judicieux d'utiliser cet argent à faire progresser la sécurité dans un autre domaine, la sécurité du transport routier dans le voisinage par exemple ?

La question que nous posons n'est pas triviale. Actuellement le contribuable dépense beaucoup d'argent pour gratter quelques décimales sur la probabilité d'accidents lors de transport de matières nucléaires. Ne serait-il pas plus judicieux de dépenser une partie de ces sommes pour améliorer le transport d'autres matières dangereuses, les produits chimiques en particulier, qui ont provoqué plusieurs centaines de morts alors qu'aucun accident de transport de matières nucléaires n'a eu jusqu'à présent la moindre conséquence.

L'objectif de notre société est l'intérêt général et la sécurité des hommes. Nous avons vu que le problème est difficile et ne connaît pas de solution parfaite. Or, le monde évolue vers de plus en plus de complexité ; les possibilités ouvertes aux hommes ne cessent de croître. Rassurons-nous cependant ; malgré de trop nombreuses bavures, la sécurité technique est également en progrès.
Mais tout accident est un drame humain, tout accident est profondément indésirable. Il importe de continuer à œuvrer tenacement pour réduire le risque, autrement dit la probabilité de catastrophe.
La complexité inhérente au problème, les interactions profondes entre les aspects techniques, psychologiques, passionnels, politiques, sociaux, économiques et nécessairement juridiques font partie des données auxquelles il faut faire face. Nous avons vu par quelques exemples que des actions diverses, mêmes très bien intentionnées, peuvent avoir des effets pervers.
Lorsque, malheureusement, un drame s'est produit, inévitablement les passions s'attisent et la sérénité devient plus difficile. C'est pourquoi il paraît essentiel que se développe "à froid" une compréhension mutuelle, constructive mais sans complaisance réciproque, entre tous les acteurs concernés, notamment entre le monde juridique et le monde technique. Dans l'intérêt général, peuvent en résulter peut-être, à plus ou moins long terme, des évolutions, tant des approches techniques que du droit et de ses interprétations.

Ce chapitre a été rédigé avec le concours de Pierre Lecomte, membre de l'Académie de l'Air et de l'Espace.

d'après GOSCINNY et UDERZO

Il n'y a pas hélas de potion magique pour rendre les opérateurs humains infaillibles et les accidents impossibles.

CHAPITRE 16

Il existe dans le mur du déterminisme, une faille dont la constante de Planck mesure l'épaisseur.

Louis de Broglie

C'est une erreur de croire que toutes les fautes ne sont que des erreurs, mais c'est une faute lourde d'estimer que toutes les erreurs sont des fautes.

Frère Jehan d'Héturbine (1606 – 1669)

POUVONS-NOUS CONCLURE ?

Nous venons de montrer que l'homme est faillible, mais que nous ne pouvons éviter sa présence dans la conduite des grands systèmes.

La probabilité pour que nous soyons démentis, sur ce dernier point, de notre vivant, est suffisamment faible pour entrer dans le domaine du risque acceptable.

Il nous faut alors lutter pour éviter, dans la mesure du possible, de mettre les opérateurs humains dans des conditions favorisant leurs faiblesses. Nous disposons de méthodes de conception des systèmes et d'une méthode de critique de cette conception, assurée par le Retour d'Expérience. Nous devons utiliser ces méthodes si nous voulons améliorer la sécurité qui, dans l'état actuel de la technologie, plafonne fâcheusement depuis quelques années du fait des conséquences des erreurs humaines. Notons toutefois une amélioration, sans doute encore insuffisante mais réelle de la sécurité du transport aérien due à l'utilisation raisonnée des automatismes sur les avions de la dernière génération dite des "glass cockpit".

Une **double démarche** s'impose. Nous allons nous répéter mais nous avons déjà fait remarquer qu'il faut plus d'un coup de marteau pour enfoncer un clou.

Nous devons tout d'abord détecter les défauts de chaque système en cause et trouver des remèdes pour les éliminer ou du moins les réduire. Nous diminuerons d'autant les probabilités d'apparition de conditions néfastes conduisant l'homme à l'erreur.

Il nous faut ainsi

- définir clairement les objectifs des tâches confiées à chacun et s'assurer qu'ils sont bien compris et connus,
- répartir clairement les responsabilités d'exécution des tâches entre les opérateurs et s'assurer que cette répartition est bien comprise et connue de tous,
- fournir aux opérateurs les moyens, en hommes et en matériels, suffisants pour l'exécution des tâches qui leur sont confiées
- fournir des procédures simples, faciles à choisir, couvrant le maximum de cas prévisibles et s'assurer qu'elles sont bien comprises et connues de tous.
- concevoir des machines sur des principes ne risquant pas de conduire à des situations dangereuses à l'insu des opérateurs.
- concevoir des postes de travail respectant les règles de l'ergonomie "mécanique", c'est-à-dire tenant compte des caractéristiques "physiologiques et anatomiques" des opérateurs.
- concevoir des postes de travail respectant les règles de l'ergonomie "cognitive", c'est-à-dire tenant compte des caractéristiques "socio-psychologiques" des opérateurs.
- former correctement les opérateurs en leur permettant d'acquérir, et les connaissances générales de base et les connaissances particulières nécessaires à la compréhension du fonctionnement des systèmes à contrôler.
- vérifier l'acquisition de connaissances réelles et non formelles des opérateurs.
- fournir aux opérateurs des documents faciles à manipuler et exempts d'erreurs matérielles,
- fournir aux opérateurs des documents faciles à consulter afin d'y trouver simplement et rapidement les informations nécessaires, aussi complètes et exactes que possible.
- enfin modifier les règlements s'ils se révèlent inappropriés à l'usage.

Cette démarche, fondamentale, se révèle néanmoins insuffisante. Nous réduisons ainsi la probabilité de voir un opérateur commettre une erreur, mais cette probabilité reste encore trop élevée si **une seule erreur**, possible et prévisible, **a une catastrophe pour conséquence**.

C'est à ce niveau que se situe la deuxième démarche.

C'est le même raisonnement qui a conduit à faire en sorte qu'une défaillance unique d'un système ne conduise pas à une catastrophe, car nous ne pouvons démontrer que la panne unique a une probabilité suffisamment basse pour être négligée. La solution pour les systèmes réside dans la redondance dissemblable.

Il nous faut entreprendre une démarche analogue pour l'erreur unique de l'opérateur. Les moyens pour satisfaire cette exigence sont abondamment décrits dans le chapitre 12. N'y revenons pas.

Ces deux démarches, réduction des probabilités d'apparition de circonstances favorisant l'erreur, traitement des erreurs humaines uniques causes de catastrophes, sont à la base de toute action d'amélioration de la sécurité des systèmes pilotés.

Verrons-nous ou plutôt, nos enfants ou petits enfants verront-ils un jour des systèmes entièrement automatiques sans aucune intervention humaine. Nous l'avons dit en début de cette conclusion, nous n'y croyons guère bien que chacun sache qu'il est très difficile de faire des prévisions. N'oublions pas que "prévoir c'est remplacer l'incertitude par l'erreur !" comme l'a rappelé un spécialiste de la science dite Prospective.

Pour terminer cet ouvrage sur un ton aussi léger que celui utilisé en l'entamant, ce qui n'en interdit pas le sérieux, évoquons les ouvrages de Science Fiction.

Ceux-ci nous présentent deux types de robots, d'un côté les machines énormes, omniscientes et omnipotentes, capables de résoudre tous les problèmes, de tout prévoir mais asservissant l'humanité et de l'autre les androïdes, bâtis à l'image de l'humain et risquant, eux aussi, d'asservir les hommes et même de les éliminer.

Nous ne sommes pas aussi pessimistes, ce qui ne nous empêche pas de nous divertir à la lecture de ces histoires qui valent bien les contes de fées de notre enfance.

Nous savons que la machine capable de tout prévoir est une utopie pour des raisons profondes et tout aussi incontournables que la croissance inéluctable de l'entropie interdisant le mouvement perpétuel ou que le principe d'incertitude d'Heisenberg. La non-linéarité des modèles mathématiques conduit à l'impossibilité de prévision à terme, toute imprécision, aussi minime soit elle sur les données initiales, se traduisant par une modification des conditions finales, imprévisible a priori et sans commune mesure avec l'écart initial (les fameux attracteurs étranges ou le chaos déterministe). Ainsi ne disposerons-nous jamais de machines capables de tout prévoir et devrons-nous nous en remettre aux sentiments, autrement dit au "pifomètre" de l'homme pour prendre des décisions, même si ces décisions sont appuyées par des informations venant d'ordinateurs puissants, dotés de grandes mémoires et capables de traiter beaucoup d'informations en peu de temps. C'est l'homme et l'homme seul qui décidera de planter cette année du maïs dans son champ plutôt que du sorgho, car aucun ordinateur ne sera en mesure de prévoir la pluviométrie précise en août entre le dix et le trente du mois et de donner les cours comparatifs de l'euro, du dollar et du yen en septembre. Tout au plus pourra-t-il consulter des tables de probabilités, tirées de modèles météorologiques et économiques et "moulinées" par des ordinateurs tout aussi puissants qu'imbéciles.

Quant aux androïdes, nous n'en voyons pas l'utilité. Pourquoi imiter l'homme, totalement imparfait sur le plan mécanique, ne disposant que de deux bras à mobilité très limitée, de deux jambes le forçant à un équilibre précaire, de deux yeux ne regardant que dans une seule direction !

Nous n'avons trouvé qu'un seul roman justifiant le robot androïde, "Les femmes de Stepford" d'Ira Levin. Les hommes de la petite ville américaine de Stepford remplacent leurs épouses par des copies robotisées, un peu améliorées sur le plan physique, excellentes cuisinières, dociles, toujours disponibles et peu bavardes. Ces robots sont une amélioration du complexe mixer - machine à laver - poupée gonflable. Je doute que la meilleure moitié de l'humanité apprécie cette robotisation intempestive !

Il est enfin amusant de noter que le célèbre auteur de science fiction Isaac Asimov ait cru bon créer les lois de la robotique pour limiter les risques de domination des robots sur l'humanité, risques concrétisés par ce qu'il

nomme le complexe de Frankenstein, la peur de voir la créature se retourner contre son créateur. Il n'a commis qu'une seule erreur en créant ses trois lois et en rajoutant une quatrième à la fin de son œuvre, c'est de les rendre déterministes et non pas probabilistes. Cette erreur est d'ailleurs très bénéfique puisque toutes ses nouvelles, pour notre plus grand plaisir, reposent sur les contradictions qui en résultent et qui laissent les robots coincés dans une situation les empêchant de prendre toute décision.

Il est par ailleurs significatif que dans le dernier roman achevant "Fondation", il montre le vieux robot Daneel R. Olivaw, conçu quelques millénaires plus tôt, ne pouvant se résoudre à prendre la décision de détruire une planète avec tous ses habitants pour sauver le reste de l'humanité dispersé dans toute la galaxie. Le robot choisit le suicide et laisse la décision à un humain, car seul un humain peut prendre une telle responsabilité reposant sur des critères qualitatifs et une déontologie non programmable dans une machine.

L'erreur humaine est aujourd'hui suffisamment bien connue, nous disposons maintenant d'outils pour la combattre et pendant longtemps encore nous ne pourrons nous passer de l'homme pour contrôler les machines.

Nous pouvons, nous devons réduire la fréquence d'apparition des erreurs humaines, en limiter les effets nocifs et utiliser les qualités irremplaçables de l'homme pour améliorer la sécurité de notre monde et ne plus considérer les catastrophes technologiques comme une malédiction inévitable et imparable.

Nous devons nous garder d'adopter une attitude laxiste vis-à-vis des fautes commises mais nous devons également éviter de transformer toutes les erreurs en fautes et chercher systématiquement "le coupable" pour chaque catastrophe. L'amélioration de la sécurité passe par l'abandon du juridisme aveugle et l'adoption de méthodes d'analyse constructive des incidents et des accidents en service pour en établir les causes profondes et non pour dénoncer des "responsables coupables".

d'après HERGÉ

ANNEXE 1

Sécurité. Situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger, à aucun risque d'agression physique, d'accident, de vol, de détérioration.
Cette installation présente une sécurité totale.

Petit Larousse

OBJECTIFS DE SECURITE

Toute étude de sécurité doit préciser quels sont les événements redoutés dont on cherche à minimiser la probabilité d'apparition et quels sont les types d'agressions qui peuvent provoquer ces événements redoutés. A titre d'exemple, lors d'une étude de sécurité sur un navire destiné à effectuer une course autour du monde il faudra, parmi les événements redoutés placer les avaries de coque ou de flotteur et parmi les types d'agressions les objets dérivant en surface. Bien entendu d'autres événements redoutés et d'autres types d'agressions doivent être retenus, mais il est nécessaire de bien préciser toutes les rubriques retenues en tenant compte du fait que les moyens de sécurité à mettre en place peuvent être très différents suivant les choix, car certains objectifs peuvent conduire à des solutions contradictoires. Par exemple devra-t-on privilégier le fait de ne pas perdre la course (événement redouté "perte de l'image de marque") ou le fait de parvenir à destination sans pertes de vies humaines et sans blessures pour l'équipage ?

Les listes suivantes ne prétendent pas être exhaustives !

⇨ Événements redoutés

- ⇨ **Pertes de vies humaines**
  - → Personnel de l'entreprise (accidents du travail)
  - → Personnes transportées, usagers
  - → Personnes hors de l'entreprise (riverains, personnes survolées, etc.)
- ⇨ **Dégradations ou pertes de matériels de l'entreprise**
  - → Bâtiments
  - → Mobilier
  - → Matériels roulants, volants, flottants, etc.
  - → Machines
  - → Outillages
  - → Matériels informatiques
  - → Matériels et Réseaux de communication
  - → Archives
- ⇨ **Atteinte par l'entreprise, à l'environnement extérieur et/ou intérieur à l'entreprise**
  - → Pollution
  - → Saleté, immondices
  - → Corrosion, dégradation, destruction de matériels (voir liste ci-dessus)
  - → Bruit
  - → Bang supersonique
  - → Pollution électromagnétique
- ⇨ **Dégradations ou pertes de logiciels de l'entreprise**
  - → Logiciels spécifiques aux systèmes utilisés par l'entreprise
  - → Logiciels de gestion de réseaux
  - → Bases de données
  - → Archives
- ⇨ **Dégradation, perte ou vol du Savoir Faire de l'entreprise**
- ⇨ **Pertes de clientèle**
  - → par diminution de la qualité du service rendu par l'entreprise
  - → par détournement de la clientèle par la concurrence
  - → par évolution des besoins de la clientèle
- ⇨ **Pertes financières**
- ⇨ **Perte de l'image de marque**

⇨ Types d'agression

⇨ Agressions internes au système

→ **Défaillances du personnel**
- erreur humaine, problème de fiabilité des hommes
- incapacité physique ou mentale des opérateurs

→ **Défaillances du matériel** (pannes, problème de fiabilité du matériel)
→ **Rayonnement électromagnétique des systèmes électroniques**
→ **Fuites de produits toxiques** transportés, produits, transformés, etc.
→ **Incendie**
→ **Mouvements sociaux**

⇨ Agressions externes au système

→ **Phénomènes naturels**
- → Tremblements de terre
- → Vents et Tempêtes
  - rafales de vent latérales pour les véhicules terrestres
  - rafales de vent, turbulence, cisaillements de vent pour l'aéronautique
  - état de la mer pour la navigation maritime ou les installations off shore
  - rafales de vent pour les bâtiments terrestres, les navires ou les installations off shore
- → Inondations (routes ou pistes d'atterrissage, favorisant l'aquaplanage)
- → Pluie, neige, verglas, grêle, slush, congères, etc.
- → Sécheresse réduisant les possibilités d'alimentation en eau des installations
- → Températures extrêmes (effets sur les hommes et les matériaux)
- → Perturbations électromagnétiques (orages, rayonnement cosmiques, etc.)

→ **Obstacles liés à des phénomènes naturels ou des activités humaines**
- → déformations de la chaussée (nids de poule, ornières, gravillons, etc.)
- → chutes de pierres ou d'objets sur la route, la voie ferrée
- → épaves, objets dérivant sur l'eau
- → débris de satellites ou de lanceurs en orbite

→ **Malveillance**
- → Sabotage
- → Terrorisme
- → Guerre
- → Manifestations
- → Vol
- → Vandalisme
- → Virus informatiques
- → Espionnage industriel
- → Espionnage militaire

→ **Concurrence**
- → Légale
- → Illégale (contrefaçon, dumping, etc.)

→ **Activités industrielles extérieures à l'entreprise**
- → Pollution, corrosion
- → Saleté, immondices
- → Produits toxiques
- → Rayonnement électromagnétique des installations industrielles
- → Rayonnement électromagnétique des systèmes de production et de transport d'énergie électrique

→ Défaillance d'un fournisseur
- énergie (carburant, électricité, etc.)
- information (téléphone, réseaux informatiques, etc.)
- matériel (pièces de rechange, matériaux, etc.)
- personnels intérimaires
- sous-traitance

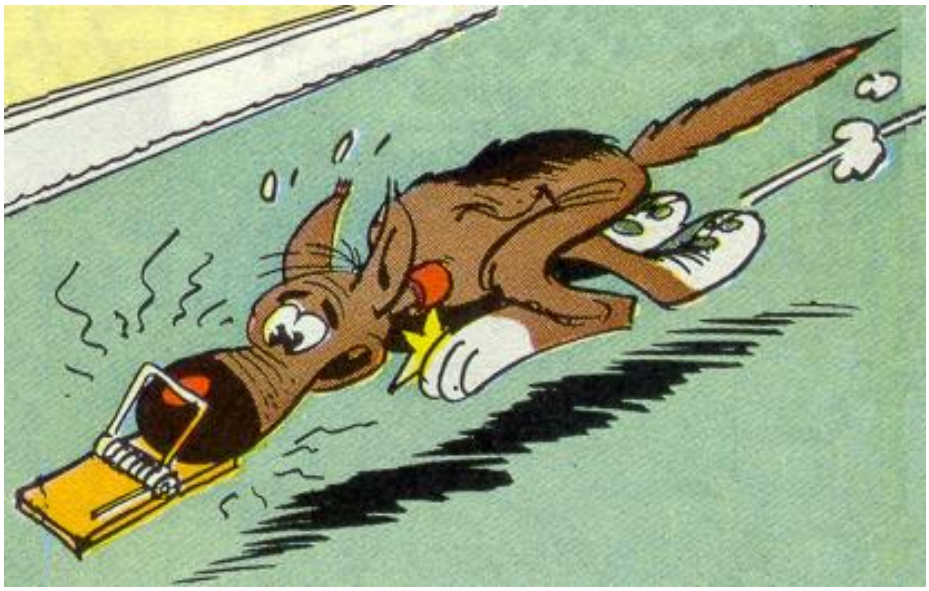
→ **Activités humaines extérieures à l'entreprise** (sans désir de nuire)
→ Action intempestive des usagers
→ Action intempestive des riverains
→ Rayonnement électromagnétique des ordinateurs (passagers)

→ **Activités animales**
→ Microbes, virus et vecteurs de maladies
→ Animaux venimeux
→ Insectes nuisibles (mouches, moustiques, poux, puces, termites, etc.)
→ Rongeurs
→ Animaux aquatiques obstruant les canalisations
→ Animaux de grande taille
- bestiaux et gros gibiers pour les transports terrestres
- oiseaux pour les transports aériens
- cétacés pour les transports maritimes
- bêtes féroces

→ **Activités végétales**
→ Algues, moisissures, mousses, etc.
→ Plantes agressives (ronces, orties, etc.)
→ Plantes envahissantes (lierre, racines, lianes, forêt vierge, plantes aquatiques, etc.)
→ Plantes vénéneuses

→ **Activités "étatiques"**
→ Réglementations
→ Justice
→ Impositions diverses

→ **Activités des groupes de pression**



D'après Morris et Goscinny

Exemple d'événement redouté et de type d'agression non cités dans cette Annexe démontrant que les listes sont loin d'être exhaustives.

ANNEXE 2

Les statistiques montrent que dans 80 pour cent des cas les accidents ont l'erreur humaine pour origine. Les 20 pour cent restants ont la même origine, mais c'est moins grave car ils sont moins nombreux.

QUELQUES CONSIDÉRATIONS SUR LES PROBLÈMES DE SÉCURITÉ

DEMONSTRATIONS DE SECURITE

Les objectifs généraux de sécurité que l'on impose aux grands systèmes se traduisent, entre autres, par des objectifs particuliers de fiabilité au niveau des fonctions assurées par chacun des sous-systèmes. Parmi les sous-systèmes, il ne faut pas oublier les opérateurs humains appelés à assurer de multiples fonctions, certaines en secours de systèmes automatiques.

Pour certaines fonctions critiques, les probabilités maximales de perte de la fonction peuvent ainsi être fixées à des valeurs aussi basses que 10^{-9} ou 10^{-10} par heure.

Or pour démontrer, par des essais, que la probabilité de défaillance d'un système est inférieure à 10^{-n} par heure (avec un niveau de confiance de 0,9), il est nécessaire d'effectuer $2,3.10^{n}$ heures d'essais sans rencontrer la défaillance.

Le chapitre suivant de cette Annexe précise la notion de niveau de confiance et l'origine de cette valeur de $2,3.10^{n}$.

Ainsi la démonstration directe de 10^{-9} par heure exigerait d'effectuer 262 560 ans d'essais continus !

On réalise ainsi que seules sont accessibles, par des essais directs, les probabilités de l'ordre de 10^{-3} par heure qui n'exigent que 100 jours environ d'expérimentation.

Il est toutefois nécessaire d'effectuer ces essais dans des conditions réalistes, respectant les conditions d'emploi et d'ambiance réelles, ce qui n'est pas toujours facile (l'impesanteur est bien évidemment irréalisable en laboratoire, pour des durées d'essais supérieures à quelques secondes). La plus grande prudence est donc nécessaire pour l'interprétation des essais de laboratoire.

Dans certains cas, l'expérience acquise sur des matériels en service permet d'estimer des probabilités de défaillance un peu inférieures à 10^{-3} par heure, mais il est bien difficile de démontrer avec un niveau de confiance raisonnable, des valeurs inférieures à 10^{-5} par heure (rappelons que cette valeur exige l'accumulation de 26 ans d'expérience continue).

En définitive, la démonstration de 10^{-9} ou de 10^{-10} ne peut se faire directement par essais. Il est nécessaire de la faire reposer sur le calcul.

Si la fonction est assurée par deux systèmes et si ces deux systèmes sont *indépendants*, la probabilité de perte de la fonction est le produit des probabilités de défaillance de chacun des systèmes.

On voit ainsi apparaître la nécessité de tripler au moins les systèmes pour pouvoir démontrer 10^{-9}, puisque la probabilité de défaillance d'un seul système ne peut être démontrée inférieure à 10^{-3}.

La redondance des systèmes est donc une nécessité, non pour *assurer* la fiabilité d'un système, mais pour la *démontrer*.

Il se peut en effet que la fiabilité réelle d'un seul système soit 10^{-7} et qu'ainsi la probabilité de perte de la fonction par le système redondé soit de 10^{-21}. Mais nous sommes dans l'incapacité de le démontrer. Force nous est donc de tripler le système.

Dans certains cas où la redondance est pratiquement impossible, en particulier pour les pièces principales de structure, la démonstration de fiabilité directe est alors également impossible.

La démonstration de la sécurité repose dans ce cas sur des calculs aussi précis et représentatifs que possible, sur l'utilisation de marges pour couvrir les incertitudes, et en définitive sur l'intime conviction du concepteur qui s'appuie sur l'expérience accumulée par ses prédécesseurs et lui-même.

La démonstration de l'objectif de fiabilité par la redondance suppose l'*indépendance réelle* des composants, sinon la règle de multiplication des probabilités élémentaires n'est pas valable.

L'indépendance physique des systèmes est facile à assurer dans son principe. Il suffit de vérifier que le fonctionnement de chacun ne dépend pas d'un seul autre et même système (en particulier sources d'énergie ou alimentations en fluides), créant ce que l'on a coutume d'appeler un *mode commun*.

Par ailleurs, on notera que la défaillance d'un système n'est pas due à un phénomène réellement aléatoire. On traite l'apparition des défaillances comme des phénomènes aléatoires, mais ceci n'est qu'un modèle mathématique commode. En réalité, une défaillance provient du dépassement d'une limite pour l'un des composants du système, dépassement provenant soit des conditions d'emploi fluctuant au cours du temps, soit d'une caractéristique anormale du composant.

Or si une défaillance apparaît sur l'un de deux systèmes, de même conception, constitués de composants fabriqués à des instants voisins avec la même méthode et les mêmes matériaux de base, il y a de grandes chances, les mêmes causes produisant les mêmes effets, pour que la même défaillance se produise sur le même composant de l'autre système.

Ainsi deux systèmes "identiques" ne sont-ils pas réellement indépendants.

La démonstration de sécurité nécessite donc d'utiliser des systèmes non seulement *redondants* mais également *dissemblables* pour assurer une fonction donnée.

Cette conclusion est encore plus importante lorsqu'il s'agit de calculateurs. Il est évident que le même logiciel fonctionnant sur plusieurs calculateurs en parallèle constitue une source de dépendance irréfutable.

Une défaillance du matériel sur l'un des calculateurs identiques a de grande chance de se produire sur les autres. Mais une défaillance du logiciel se produira instantanément sur tous les calculateurs.

On propose quelque fois de faire réaliser le logiciel par plusieurs programmeurs indépendants, en espérant qu'ils ne commettront pas les mêmes erreurs. La formation et les méthodes des programmeurs sont déjà des sources de dépendance. Mais le cahier des charges est une autre source, encore plus importante, de dépendance (erreur dans la logique, oubli de cas particuliers..).

La difficulté provient du fait que l'on demande aux calculateurs d'assurer deux fonctions, une fonction d'optimisation pour l'économie du système et une fonction de sécurité. La défaillance de la fonction de sécurité, non seulement n'assure pas l'économie, mais également ne permet pas de continuer la mission.

La solution consiste donc à séparer ces fonctions. Un premier groupe de calculateurs est doté d'un logiciel sophistiqué (donc sujet à erreurs) pour assurer l'optimisation. Leur redondance n'est justifiée que pour couvrir les défaillances du matériel.

Un deuxième groupe de calculateurs, de conception différente du premier groupe, est doté d'un logiciel beaucoup plus simple destiné seulement à ramener le système dans un état sûr en cas de défaillance du logiciel du premier groupe. Ce logiciel, plus simple et par là même probablement moins coûteux à établir, est moins sujet à erreurs et son cahier des charges étant différent du cahier des charges du premier groupe, il y a moins de chances pour qu'une erreur soit commune aux deux logiciels. Cela est encore plus vrai si le deuxième groupe est constitué de calculateurs analogiques et le premier de calculateurs digitaux.

Bien entendu, dans le cas d'une redondance du seul matériel, il se peut que la fiabilité réelle du logiciel soit suffisante. La démonstration directe en est impossible, mais le fait d'utiliser des langages de programmation évolués, des méthodes éprouvées d'écriture de programme, des équipes bien préparées peut entraîner l'intime conviction du responsable de la conception.

L'expérience acquise dans le domaine de l'informatique en évolution exponentielle est-elle du même ordre de grandeur que celle acquise en mécanique et en structure ? Nous en doutons.

Une autre façon d'assurer la redondance d'un système automatique (matériel et logiciel), consiste à le doubler par un opérateur humain. Il est évident que les erreurs de logiciel du système et du cerveau de l'opérateur ont peu de chances d'être communes (sauf si les modèles de comportement du système à contrôler sont les mêmes, pour le concepteur du logiciel et pour l'opérateur humain). Bien entendu, il est nécessaire de tenir compte des défaillances particulières de l'opérateur humain pour en estimer la fiabilité et en déduire la fiabilité du "composite" automatisme - opérateur.

LES ESTIMATIONS DE FIABILITÉ.

L'évaluation de la fiabilité d'un matériel peut se faire par des essais systématiques en laboratoire, par examen du fonctionnement de ce matériel en service réel ou encore par comparaison avec des matériels existants.

Nous n'étudierons ici que l'évaluation par essais en laboratoire.

Pour rendre plus accessible le raisonnement, nous ne chercherons pas à évaluer directement la probabilité de défaillance d'un matériel, mais sa durée de vie moyenne et nous reviendrons ultérieurement sur la relation durée de vie, probabilité de défaillance.

Il est possible pour un matériel donné de mesurer sa masse, sa consommation en énergie, son volume, sa bande passante, d'une façon générale tout paramètre caractérisant ses performances. Il est également possible de mesurer sa durée de vie en le faisant fonctionner en laboratoire et en notant le temps d'apparition de la défaillance conduisant à la perte de la fonction assurée.

Pour faciliter le raisonnement, nous supposerons que l'apparition d'une défaillance est du type tout ou rien, c'est-à-dire que la première défaillance conduit à la perte de la fonction (sans faire appel à la notion de fonctionnement dégradé qui compliquerait inutilement la notion de mesure de la durée de vie). Ainsi la durée de vie est un paramètre de performance mesurable analogue aux premiers cités. Par contre sa connaissance est sans intérêt puisque qu'elle n'est effective qu'une fois le matériel hors d'usage.

Nous cherchons donc, non à mesurer la durée de vie d'un exemplaire d'un matériel donné, mais à évaluer la durée de vie d'un exemplaire quelconque de ce matériel, construit en série, avant la mise en service de cet exemplaire, en faisant des mesures sur un échantillon.

Cette démarche peut se faire également pour d'autres performances du matériel, pour la masse, le volume, la consommation, etc. On peut ainsi désirer obtenir la masse moyenne d'un matériel en faisant la mesure de la masse de quelques matériels d'un échantillon. Mais notons bien qu'il ne s'agit pas de mesurer la masse moyenne des matériels de l'échantillon; il s'agit, à partir des mesures des masses des matériels de l'échantillon, de fournir une estimation raisonnable de la masse moyenne des matériels de même type sur lesquels nous n'avons pas fait de mesure.

Cette démarche est la même pour l'estimation de la durée de vie. Il s'agit, à partir de mesure de la durée de vie observée sur quelques matériels en laboratoire, d'en déduire une estimation de la durée de vie moyenne des matériels qui seront mis en service dans des conditions réelles d'emploi. La seule différence avec l'estimation de la masse moyenne ou de la consommation moyenne est que les matériels utilisés pour les essais sont nécessairement détruits en fin d'essai.

On retrouve le problème d'étude des allumettes. Rien ne sert de savoir qu'une allumette particulière s'est bien allumée. Par contre il est intéressant, après avoir testé un lot d'allumettes, d'en déduire qu'elle est la probabilité de bon fonctionnement d'une allumette quelconque de la même fabrication utilisée dans les mêmes conditions d'environnement.

La première précaution à prendre pour les essais de laboratoire est de réaliser des conditions de fonctionnement, ambiance (température, pression, vibrations, humidité, etc.), mise en service et arrêt, tension d'alimentation, etc. reproduisant au mieux les conditions réelles d'emploi.

Nous supposerons ces conditions réalisées pour les essais d'un matériel donné.

De nombreuses méthodes d'essais peuvent être utilisées:

- faire fonctionner un seul système jusqu'à l'apparition de la première défaillance après n heures,
- faire fonctionner q matériels identiques et noter le nombre n d'heures de fonctionnement à l'apparition de la défaillance du r-ième matériel, sans remplacer les matériels défaillants ou en remplaçant les matériels défaillants,
- faire fonctionner q matériels identiques, attendre n heures et constater le nombre r de matériels en défaillance (avec ou sans remplacement des matériels défaillants), etc.

En définitive nous avons mesuré un certain nombre de valeurs de durée de vie pour quelques matériels d'un échantillon.

Le statisticien considère que la durée de vie T d'un matériel est une variable aléatoire et, ayant mesuré quelques valeurs sur un échantillon, il essaie de caractériser cette variable aléatoire en donnant sa valeur moyenne entre autres, sa fonction de répartition, etc.

Ainsi, pour une méthode d'essai donnée, une méthode donnée du choix des matériels constituant l'échantillon, et moyennant quelques hypothèses sur les lois de probabilités régissant la variable aléatoire T, le calcul statistique détermine trois valeurs T_e, ΔT_e et P, et permet d'affirmer que la valeur moyenne du paramètre T peut être estimée à $T_e \pm \Delta T_e$, avec une probabilité P de ne pas se tromper. Lorsque P se rapproche de 1 on a de plus en plus confiance dans les résultats, d'où le nom de niveau de confiance donné à la variable P.

Si ultérieurement on met en service un matériel X choisi au hasard, on observera une durée de vie T de ce matériel. On peut alors affirmer, avant mise en service du matériel X, que la valeur T que l'on observera, a la probabilité P d'être à l'intérieur de la bande $T_e \pm \Delta T_e$.

Il se peut que les essais sur le premier échantillon se soient déroulés avec des matériels "anormaux" conduisant à une mauvaise estimation de T_e et de la marge ΔT_e. Il se peut aussi que le matériel X en service soit également un matériel "anormal". La probabilité de s'être trouvé, par "hasard" dans ces cas "anormaux" est 1- P.

Il est évident que plus on cherche à définir la marge ΔT_e avec une probabilité P grande de ne pas se tromper, plus, pour un essai donné, la plage ΔT_e est grande. On se doute aussi que si l'on augmente le nombre des essais, on diminue ΔT_e pour P donné ou que l'on augmente P pour ΔT_e donné.

En définitive chaque estimation T_e de la durée de vie doit s'accompagner d'une marge ΔT_e et d'un niveau de confiance P.

La durée de vie moyenne T_m étant ainsi estimée par T_e, on peut traduire ce résultat par une probabilité de défaillance par heure de fonctionnement. Il est nécessaire de faire quelques hypothèses supplémentaires (par exemple la probabilité de défaillance ne dépend pas du temps). Des calculs classiques de probabilité, que nous développerons dans le chapitre suivant, permettent ainsi de calculer, connaissant T_e, ΔT_e, la probabilité p_e de défaillance par heure estimée pour le matériel étudié. Pour fixer les idées, on peut ainsi dire que si l'on a observé un temps T_m de 1000 heures, la probabilité p_e est de 1/1000 par heure.

Là encore la valeur p_e doit être présentée accompagnée d'une marge Δp_e (calculée à partir de la marge ΔT_e) et du niveau de confiance P.

Dans le cas particulier où la méthode d'estimation de p_e consiste à faire fonctionner des matériels identiques pendant $2{,}3\ 10^n$ heures cumulées sans rencontrer de défaillance, le calcul, compte tenu d'hypothèses sur la loi d'apparition des défaillances, permet d'affirmer que la probabilité p_e est inférieure à 10^{-n} par heure (la marge est alors de 10^{-n} à 0) avec un niveau de confiance de 0,9.

Ces chiffres sont liés à la méthode d'essai et à la loi supposée d'apparition des défaillances et à quelques hypothèses supplémentaires. D'autres valeurs sont à retenir avec des méthodes différentes et, bien entendu, avec des niveaux de confiance différents.

Nous retiendrons toutefois que l'ordre de grandeur du nombre d'heure d'essais est de $k.10^n$ (k entier entre 1 et 10), pour démontrer une probabilité p_e inférieure à 10^{-n} par heure avec un niveau de confiance P de l'ordre de 0,9.

Nous avons supposé jusqu'ici que l'on cherchait à estimer la probabilité p de défaillance d'un matériel entièrement nouveau pour lequel on ne dispose d'aucun renseignement complémentaire concernant sa fiabilité. Le nombre d'essais nécessaire pour la démonstration d'une probabilité p de défaillance donnée n'est plus le même que celui donné ci-dessus lorsque l'on dispose de résultats d'essais en laboratoire ou de résultats opérationnels ayant déjà conclu à une probabilité démontrée p'. Le passage de p' à une nouvelle estimation p repose sur des considérations qui sortent du cadre nécessairement limité de cet exposé, mais les méthodes et conclusions sont bien connues des statisticiens.

En conclusion, nous retiendrons que des méthodes de mesure statistiques portant sur un échantillon de matériels (détruits en fin d'essai) permettent d'affirmer que la probabilité de défaillance d'un matériel de série, mis en service opérationnel, sera inférieure à une valeur p et ceci avec une probabilité P, dite niveau de confiance, de voir cette affirmation confirmée en utilisation.

Une seconde conclusion s'impose. Si au cours de l'utilisation réelle d'un système, dont on a estimé, par essai de laboratoire, la durée de vie moyenne à 1000 heures, on observe une défaillance au bout de 10 heures seulement, il ne faut pas en déduire que l'on est face à un cas d'espèce, que l'on a eu la malchance de tomber sur un mauvais matériel, etc. En effet, la probabilité d'observer une défaillance au bout de 10 heures sur un matériel de durée de vie moyenne 1000 heures, n'est que de 0,01. Cela montre bien qu'il ne faut pas négliger cet avertissement et faire quelque chose (modifier le matériel, modifier ses conditions d'ambiance et d'emploi, etc.)

LA LOI DE POISSON.

Temps moyen d'apparition d'une défaillance

Nous supposerons que la probabilité d'occurrence de la défaillance du système étudié est indépendante du temps. Autrement dit, quel que soit l'instant t, la probabilité d'observer une défaillance entre l'instant t et l'instant t + dt est p.dt où p est une constante. On suppose que la défaillance est caractérisée par le passage brutal, à un instant donné, de l'état "fonction assurée" à l'état "fonction non assurée".

Soit Q_t la probabilité pour que la défaillance n'ait pas été observée avant l'instant t et $Q_t + dQ$ la probabilité pour que la défaillance n'ait pas été observée avant l'instant t + dt.

Pour que la défaillance n'ait pas été observée à l'instant t + dt, il faut qu'elle n'ait pas été observée jusqu'à l'instant t (probabilité Q_t de cet événement) et qu'elle n'ait pas été observée entre les instants t et t + dt (probabilité 1- p.dt de ce dernier événement, puisque p.dt est la probabilité d'apparition de la défaillance entre t et t + dt). La probabilité de la conjonction de ces deux événements est donc le produit de la probabilité de chacun, soit Q_t . (1- p.dt).

En conséquence

$$Q_t + dQ = Q_t . (1- p.dt)$$

soit

$$dQ/Q_t = - p.dt$$

et

$$Q_t = e^{-pt}$$

puisque Q_t est égal à 1 à l'instant zéro.

En définitive la *probabilité P_t d'observer une défaillance avant l'instant t* est $1-Q_t$, soit

$$\mathbf{P_t = 1 - e^{-pt}}$$

(c'est la loi de POISSON).

Temps Moyen Entre Pannes et Probabilité Élémentaire de Panne

Quelle est maintenant la relation entre la probabilité élémentaire de défaillance p et le temps moyen entre défaillances ou plus simplement le temps moyen d'apparition d'une défaillance (MTBF Mean Time Between Failures) ?

A chaque temps t nous pouvons associer la probabilité $R_t.dt$ d'observer la défaillance entre le temps t et le temps t + dt. Bien évidemment cette probabilité est le produit de la probabilité Q_t de ne pas avoir observé la défaillance jusqu'au temps t par la probabilité p.dt de l'observer entre t et t + dt, soit

$$R_t.dt = Q_t.p.dt = p.e^{-pt}.dt$$

Le temps moyen d'apparition d'une défaillance est la moyenne des temps t pondérés par la probabilité R_t associée à chaque temps t.

$$T_m = \frac{\int_0^\infty t.R_t.dt}{\int_0^\infty R_t.dt} = p.\int_0^\infty t.e^{-pt}.dt = 1/p$$

Ainsi un système ayant une probabilité élémentaire de défaillance de 10^{-3} / heure a un temps moyen d'apparition de défaillance de 10^3 heures.

Calcul de la relation Temps d'essai - Niveau de confiance

Au bout de combien de temps d'essai aurons nous une probabilité 0,9 d'observer une défaillance ?

Nous cherchons le temps T pour lequel la probabilité P_t est égale à 0,9 , soit :

$$1 - e^{-pT} = 0,9$$

soit

$$\mathbf{T = - Log_e(0,1) / p = 2,3 / p = 2,3\ T_m}$$

Autrement dit, si j'observe le fonctionnement du système pendant un temps T égal à 2,3 fois le temps moyen T_m, j'ai 9 chances sur 10 d'observer une défaillance.

Une autre façon d'exprimer ce résultat consiste à dire que si je n'ai pas observé de défaillance pendant un temps T, je peux affirmer, avec une chance sur dix de me tromper (niveau de confiance de 0,9), que le système a un temps moyen avant défaillance T_m supérieur ou égal à T / 2,3. En effet, si T_m est bien égal à cette valeur T / 2,3 , j'avais 9 chances sur 10 d'observer une défaillance.

Enfin un niveau de confiance de 0,99 nécessite d'effectuer des essais pendant un temps

$$T = - Log_e(0,01) / p = 4,6 / p = 4,6\ T_m$$

La probabilité de référence 10^{-7}/heure

La probabilité de périr de mort naturelle est, de nos jours, de l'ordre de 10^{-3} par an à la naissance, passe par un minimum de 2.10^{-4}/an vers l'âge de 10 ans, retrouve la valeur initiale vers 35 ans pour atteindre 10^{-2}/an à 60 ans et 10^{-1}/an à 80.

Lorsqu'il s'agit d'exprimer le risque de périr de mort naturelle, l'année est une bonne unité de temps, car bien que nous estimant en bonne santé à un instant donné, la possibilité de tomber malade dans l'année qui suit n'est pas irréaliste.

Par contre, l'année est une unité bien trop grande lorsque nous cherchons à estimer la probabilité d'un accident de transport ou d'un accident du travail parce que nous ne passons que quelques heures consécutives dans un moyen de transport ou à un poste de travail.

Il est dans ce cas plus commode d'utiliser l'heure comme unité de temps. La probabilité de 10^{-3} par an, probabilité moyenne du risque de mort naturelle, devient alors sensiblement 10^{-7} par heure (1 an = 24 x 365 = 8760 heures).

Ainsi la **probabilité de 10^{-7} par heure est-elle une grandeur de référence** pour les risques de transport ou de travail, constituant une valeur raisonnablement acceptable pour chaque mortel. C'est cette valeur qui est communément admise pour l'établissement des règles de sécurité. Le chapitre 15 détaille les considérations éthiques et économiques qui permettent de définir cette probabilité résiduelle d'accident admissible.

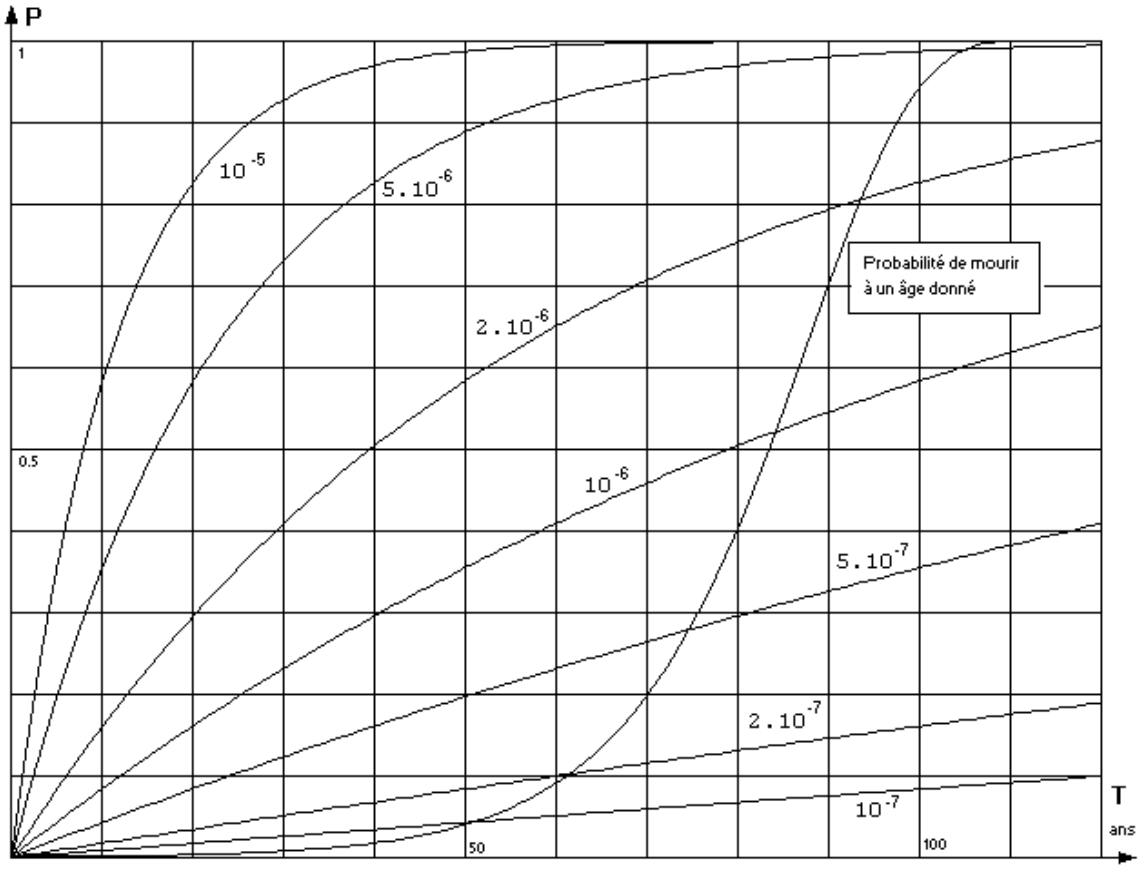
Hormis le constat que 10^{-7} par heure est la probabilité de mort naturelle aux environs de 35 ans, il est difficile d'évaluer ce que signifie un risque ayant une telle probabilité élémentaire, car ce nombre est trop faible. Pour en aider l'interprétation, nous donnons sur la figure ci-dessous la probabilité d'observer un événement ayant une probabilité élémentaire de $k.10^{-n}$ / heure (loi de Poisson) au bout d'un temps suffisamment long pour que cette probabilité soit comprise entre 0,1 et 1.

On constate ainsi qu'il faut attendre 120 ans pour que la probabilité d'observer un événement de probabilité élémentaire 10^{-7}/heure (ou 10^{-3}/an) atteigne 0,1 , ce qui confirme bien que le risque de référence est faible.

Par contre, un événement de probabilité élémentaire 10^{-6}/heure (ou 10^{-2}/an) peut être observé au bout de 80 ans avec une probabilité de 0,5.

Enfin, la courbe en S donne la probabilité de mort compte tenu de la loi de probabilité de mort naturelle décrite en début de ce paragraphe. Ainsi, à la naissance, un individu a 4 chances sur 100 de périr à 50 ans, 20 chances sur 100 de périr à 70 ans, 40 chances sur 100 de périr à 80 ans et enfin 70 chances sur 100 de périr à 90 ans. Rappelons qu'il ne s'agit ici que de mort naturelle.

La courbe de mortalité toutes causes confondues, est moins favorable.



CALCUL DE LA PROBABILITÉ DE GAGNER AU LOTO AVEC UNE GRILLE

La probabilité de tirer un bon numéro sur 49 est 1/49. Il reste alors 48 numéros disponibles. La probabilité de tirer un bon numéro sur 48 est 1/48 et la probabilité de tirer deux bons numéros est donc 1/49x48. En poursuivant le même raisonnement pour six numéros on parvient à la probabilité de 1/49x48x47x46x45x44. Mais ce raisonnement suppose que l'on a choisi les numéros dans un ordre déterminé. Or il y a une seule façon de choisir un numéro, 2 façons de choisir deux numéros, 3x2 façons de choisir trois numéros,..., 6x5x4x3x2x1 = 720 façons de choisir six numéros dans un ordre quelconque. La probabilité de tirer les six bons numéros dans un ordre quelconque est donc

$$p = 720/49x48x47x46x45x44$$

$$p = 1 / 13\ 679\ 820.$$

On vient de voir que la probabilité de périr de mort naturelle dans l'heure qui suit est de l'ordre de 10^{-7} pour un individu dans la force de l'âge.

Ainsi la probabilité de gagner au Loto avec une grille est du même ordre de grandeur que la probabilité de mourir dans l'heure qui suit !

CALCUL DE LA PROBABILITÉ D'AVOIR UN GAGNANT POUR N GRILLES JOUÉES.

La probabilité qu'une grille soit gagnante est la valeur p que nous venons de calculer. La probabilité pour qu'une grille soit perdante est donc 1 - p.

La probabilité pour que deux grilles soient perdantes est la probabilité de deux événements indépendants, la première grille est perdante, la deuxième grille est perdante.

Cette probabilité est donc le produit des deux probabilités $(1 - p)$ soit $(1 - p)^2$.

La probabilité pour que n grilles soient toutes perdantes est le produit des n probabilités 1 - p, soit $(1 - p)^n$.

La probabilité pour qu'une grille au moins soit gagnante est donc la probabilité de l'événement contraire à l'événement "aucune grille n'est gagnante". Cette probabilité est donc

$$P = 1 - (1 - p)^n$$

On remarquera que si p et n sont petits

$$(1 - p)^n \ \# \ 1 - np$$

et que par suite

$$P \ \# \ np$$

Mais cette formule, qui rejoint le bon sens (la probabilité pour que je gagne avec deux grilles est deux fois la probabilité de gagner avec une seule grille), n'est valable avec une bonne approximation que si le produit np est petit. Elle donne un résultat faux si np est grand et évidement absurde si np est supérieur à 1 !

Pour n = 13 679 820 le calcul exact donne P = 0,632 (et non 1 bien sûr !)
Pour n = 20 000 000 P = 0,768
Pour n = 60 000 000 (ou trois tirages de vingt millions de grilles), P = 0,9875

ANNEXE 3

ÉVALUATION DU RISQUE D'ERREUR HUMAINE LIÉ À LA CHARGE DE TRAVAIL

LE PROBLÈME DE L'ÉVALUATION DES CHARGES DE TRAVAIL.

Nous savons que les variations de difficulté d'une tâche ne se traduisent pas par une variation des performances de l'opérateur. Celui-ci compense une augmentation de difficulté par une augmentation de la charge de travail fournie, mais aucune manifestation extérieure ne permet de déceler le phénomène, sauf lorsque la compensation devient impossible. Si en effet la charge de travail nécessaire dépasse la charge de travail que peut fournir l'opérateur, compte tenu de son état physique et de son état psychosociologique, celui-ci abandonne une partie de la tâche et la performance s'en ressent.

On peut observer que l'opérateur répartit les paramètres à surveiller en trois classes :

- les paramètres qui relèvent de la conduite de la machine (paramètres de situation) et qui intéressent la sécurité à long terme. L'heure d'arrivée à destination pour le mécanicien du TGV, la position du terrain de destination pour le commandant de bord d'un avion de transport rentrent dans cette catégorie.
- les paramètres qui relèvent de la sécurité à court terme, c'est-à-dire ceux figurant dans la définition de l'objectif de la phase en cours. Lors du freinage à l'approche d'un carré fermé, la position de la motrice est de ce type. Lors d'une approche avant atterrissage, la position de l'avion, en écart d'altitude et en écart latéral par rapport à la trajectoire idéale, est également de ce type.
- Les paramètres qui relèvent de la sécurité instantanée. Ce sont les paramètres de pilotage ou les paramètres de fonctionnement qui risquent de franchir une limite. La vitesse du train, la température des freins entrent dans cette dernière catégorie. L'incidence, l'assiette latérale de l'avion en approche sont de ce type.

Lorsque la difficulté de la tâche augmente, l'opérateur, ne pouvant plus, au-delà d'un certain seuil, compenser par augmentation de charge de travail, abandonne progressivement la surveillance des paramètres de sécurité à long terme, puis la surveillance des paramètres de sécurité à court terme. Lorsqu'il ne peut même plus assurer la surveillance des paramètres de sécurité instantanée, la catastrophe ne tarde plus à survenir.

C'est l'abandon de la surveillance des paramètres de sécurité à court terme qui se traduit par une variation caractéristique des performances de l'ensemble système-opérateur, puisque l'opérateur ne parvient pas à atteindre l'objectif de la tâche.

Lorsqu’à la suite d'une augmentation de la difficulté, on observe une variation brusque de performance, on peut en conclure que l'opérateur a atteint la charge maximale qu'il peut fournir. Mais l'observation extérieure de l'opérateur ne permet pas de différencier des charges de travail inférieures.

Certains auteurs ont proposé de confier à l'opérateur une tâche auxiliaire aisément quantifiable et d'augmenter cette charge auxiliaire jusqu'à saturation (seul phénomène observable). La charge de travail principale serait alors d'autant plus petite qu'est grande la charge auxiliaire conduisant à la saturation.

Ce principe de mesure repose hélas sur de nombreuses hypothèses qui se sont révélées fausses. La charge de travail ne peut être représentée par un paramètre unique; les charges de travail ne sont donc pas additives; par ailleurs la charge nécessaire pour gérer le passage de la tâche principale à la tâche auxiliaire et le passage inverse n'est sûrement pas négligeable. Enfin on peut se poser la question du sens de l'opération de quantification de la charge de travail auxiliaire, qui répétons-le ne peut être représentée par un unique paramètre.

Force donc est de reconnaître que la méthode de la double tâche repose sur trop d'hypothèses erronées pour être valable.

De nombreuses tentatives ont été faites par ailleurs pour corréler des paramètres physiologiques et la charge de travail, malheureusement toujours avec l'hypothèse fausse de la représentation de la charge de travail par un paramètre unique.

Ces corrélations existent sans conteste. Diamètre de la pupille, variabilité du rythme cardiaque, etc. varient avec la charge de travail telle qu'elle est ressentie par l'opérateur. Mais ces mesures ne peuvent fournir que des indicateurs de variation de certains composants de la charge de travail (recueil de données, activité musculaire, élaboration de stratégies, etc.). En aucun cas elles ne constituent des mesures absolues et reproductibles permettant le classement des tâches. Que signifie d'ailleurs un classement d'objets caractérisés par des paramètres multiples ? Ces mesures dépendent enfin de beaucoup trop d'autres facteurs et sont en général plus sensibles à ces facteurs qu'à la charge de travail elle-même.

En définitive le seul outil disponible est l'estimation par l'opérateur lui-même de la charge de travail nécessitée par la tâche qu'il exécute, par comparaison avec les charges de travail correspondant à des tâches de référence.

L'expérience montre en effet que des opérateurs, bien au fait du problème de simulation et d'essai sur prototype ou sur machine réelle, sont capables de fournir des estimations fiables et répétitives, dans la mesure où ils ont compris qu'il s'agit d'estimer, non la charge de travail elle-même, multiforme et mal définie, mais indirectement la probabilité, dans les conditions d'essai, de commettre une erreur d'Opérabilité. Précisons que l'on ne demande pas d'estimer la probabilité d'accident, mais seulement la probabilité conditionnelle d'erreur d'Opérabilité, la probabilité d'avoir à exécuter la tâche dans les conditions d'essai résultant de l'analyse de la mission. Autrement dit, on ne demande pas à l'opérateur de dire si la tâche est acceptable ou non sur le plan sécurité. On lui demande seulement d'évaluer le risque d'erreur qu'il pourrait commettre, si on lui demandait d'exécuter réellement cette tâche, en faisant des comparaisons avec des tâches connues et bien identifiées quant aux risques qu'elles entraînent.

Ces remarques préliminaires étant admises, examinons la méthode d'évaluation.

LA MÉTHODE D'ÉVALUATION DES CHARGES DE TRAVAIL.

Définition de la tâche.

La machine à évaluer doit l'être dans le cadre bien précis d'une *opération associée*.

L'*opération associée* à une machine est définie par un *objectif global*, dans un *environnement donné* et avec des *conditions d'emploi précisées*.

Autrement dit on ne cherche pas à évaluer les risques liés à la machine elle-même, ce qui n'a aucun sens, mais les risques liés à l'utilisation de la machine dans des conditions précises. Ainsi étudier les risques causés par un marteau n'a pas de sens. Par contre, on peut estimer les risques d'utilisation d'un marteau au cours d'une opération de cloutage précise (taille du clou, matériau à clouer, présence ou non d'un autre opérateur tenant le clou, utilisation d'un autre outil pour positionner et maintenir le clou, utilisation d'un autre outil pour positionner et maintenir en place les pièces à clouer, etc.).

L'*opération associée* à la machine à étudier doit être découpée en *phases*, chaque phase étant elle-même découpée en *sous-phases*.

Une *phase* est caractérisée par un *objectif général*, une *sous-phase* est caractérisée par un *objectif élémentaire*.

Chaque objectif doit être défini avec des tolérances telles que, s'il est atteint à l'intérieur de ces tolérances, la sous phase ou la phase suivante puisse être entamée avec succès.

Pour chaque sous-phase, le manuel d'utilisation ou les procédures doivent préciser la *configuration nécessaire de la machine* (configuration géométrique, mise sur marche ou arrêt des automatismes et plus généralement des systèmes).

Pour chaque sous-phase, il faut dresser la liste des différents cas de pannes possibles et les différents cas d'environnement prévisibles pour évaluer les risques d'erreurs avec toutes les combinaisons pannes-environnement éventuelles, chaque cas constituant une *tâche*.

A chaque *tâche* on peut affecter une *probabilité* P_t, produit

- de la probabilité d'avoir à effectuer la sous-phase
- de la probabilité de la combinaison de pannes choisie,
- de la probabilité des conditions d'environnement.

La probabilité d'avoir à effectuer la sous-phase est en général égale à 1 sauf pour quelques sous-phases qui ne sont exécutées que dans des conditions particulières, comme les opérations d'urgence (par exemple freinage

d'urgence en cas de présence de bestiaux sur la voie, descente rapide en cas de perte de pression cabine). La probabilité de sous-phase est alors la probabilité d'apparition des conditions imposant l'opération d'urgence.

Évaluation du risque.

Il reste maintenant à évaluer le risque d'erreur humaine au cours de l'exécution de chacune des tâches, risque lié à la charge de travail imposée par la tâche, mais non risque d'erreurs d'autres types (maladresse, erreur de représentation, mauvaise estimation du risque, etc..) .

Après exécution, par un opérateur qualifié, d'une phase réaliste comportant plusieurs tâches, nous lui posons, pour chaque tâche, deux questions permettant de choisir l'une des six classes de risques repérées par les lettres A à F.

Par opérateur qualifié, nous entendons un opérateur qui non seulement connaît parfaitement le système essayé, mais qui connaît le "métier", c'est-à-dire les conditions réelles d'emploi des systèmes ayant des missions analogues.

Le tableau suivant résume la méthode de choix de la classe de risque.

<table>
<tr><th>Avez-vous atteint l'Objectif élémentaire de la Sous-Phase?</th><th>Le risque d'erreur, au cours de la Tâche, est-il inférieur au Risque Quotidien Maximal admissible ?</th><th>CLASSE</th></tr>
<tr><td rowspan="5">OUI</td><td rowspan="2">OUI</td><td>A</td></tr>
<tr><td>B</td></tr>
<tr><td rowspan="3">NON</td><td>C</td></tr>
<tr><td>D</td></tr>
<tr><td>E</td></tr>
<tr><td colspan="2">NON</td><td>F</td></tr>
</table>

La première question est

"Avez-vous atteint l'objectif élémentaire de la sous-phase ?"

Bien entendu l'opérateur doit connaître l'objectif de chaque sous-phase avec les tolérances associées.

Si la réponse à cette première question est **NON**, la ***tâche est classée F***.

Si la réponse est **OUI**, une deuxième question est posée :

"Le risque d'erreur au cours de cette tâche, est-il inférieur au Risque Quotidien Maximal admissible ?"

Si l'opérateur juge que les conditions d'exécution de la tâche n'entraînent pas de risque supérieur au Risque Quotidien Maximal admissible, c'est qu'***il admet d'exécuter des tâches analogues pendant toute sa carrière professionnelle en courant un risque global qu'il estime suffisamment faible pour être accepté*.**

Le risque à évaluer est soit le risque encouru par l'opérateur lui-même, soit le risque de provoquer une catastrophe entraînant perte de vies humaines et dégâts matériels importants.

Dans ces conditions, si la réponse à la deuxième question est **OUI** sans hésitation, la ***tâche est classée A.***

Si la réponse à la première question a été **OUI**, mais après hésitation, la réponse à la deuxième question ne peut être que **NON** et la ***tâche est classée E.***

Si la réponse à la deuxième question est **NON** sans hésitation, après avoir répondu OUI à la première, la ***tâche est classée D.***

Si la réponse à la deuxième question est **NON** après avoir hésité à répondre **OUI**, la ***tâche est classée C.***

Si la réponse à la deuxième question est **OUI** après avoir hésité à répondre **NON**, la ***tâche est classée B.***

Une fois une classe affectée à chacune des tâches, celles-ci sont regroupées par classes, ce qui permet de calculer la probabilité de chaque classe:

CLASSE	TÂCHE	PROBABILITÉ DE TÂCHE	PROBABILITÉ DE CLASSE
A	T_{a1}	P_{a1}	P_A
	T_{a2}	P_{a2}	
	----------	----------	
	T_{an}	P_{an}	
B	T_{b1}	P_{b1}	P_B
	T_{b2}	P_{b2}	
	----------	----------	
	T_{bn}	P_{bn}	
C	T_{c1}	P_{c1}	P_C
	T_{c2}	P_{c2}	
	----------	----------	
	T_{cn}	P_{cn}	
D	T_{d1}	P_{d1}	P_D
	T_{d2}	P_{d2}	
	----------	----------	
	T_{dn}	P_{dn}	
E	T_{e1}	P_{e1}	P_E
	T_{e2}	P_{e2}	
	----------	----------	
	T_{en}	P_{en}	
F	T_{f1}	P_{f1}	P_F
	T_{f2}	P_{f2}	
	----------	----------	
	T_{fn}	P_{fn}	

Les tâches $R_1,R_2,...,R_p$ relevant de la classe A ont été renommées T_{a1}, T_{a2},..,T_{an} de probabilités P_{a1}, P_{a2},..,P_{an}

Les tâches $S_1,S_2,...,S_q$ relevant de la classe B ont été renommées T_{b1}, T_{b2},.., T_{bn} de probabilités P_{b1}, P_{b2},.., P_{bn}

etc.

La probabilité P_A de la classe A est la somme des probabilités P_{a1}, P_{a2},..., P_{an}.

La probabilité P_B de la classe B est la somme des probabilités P_{b1}, P_{b2},..., P_{bn}.

Etc.

Pour calculer le risque lié à la sous-phase étudiée, il reste à affecter à chaque classe une probabilité de risque P_r à l'aide du tableau suivant (l'unité de temps est l'heure).

CLASSE	A	B	C	D	E	F
Probabilité Conditionnelle d'Accident par heure	10^{-11}	10^{-9}	10^{-7}	10^{-5}	10^{-3}	10^{-1}

On peut admettre qu'un opérateur moyen aura à effectuer 2000 heures par an pendant 45 ans soit 90.000 heures pendant toute sa carrière. Or la probabilité de périr dans l'heure qui suit, de mort "naturelle", est de l'ordre de 10^{-7}. Un risque est jugé acceptable si sa probabilité est du même ordre de grandeur.

Si l'opérateur admet d'effectuer une tâche de classe A pendant toute sa carrière sans courir de risque jugé excessif, cela signifie donc que la probabilité de risque attachée à la classe A est de l'ordre de 10^{-7} / 90.000 soit environ 10^{-12}/heure.

Si l'on admet que l'opérateur d'essai n'a pas une connaissance exacte de tout ce qui peut arriver à un opérateur moyen en service, on peut donc admettre que la valeur de 10^{-11}/heure est une bonne estimation de la probabilité de risque liée à la classe A.

Nous affecterons la probabilité 10^{-1}/heure à la classe F. Elle est en effet très voisine de 1 puisque l'opérateur d'essai n'a pas réussi à atteindre l'objectif de la sous phase dans les conditions imposées par la tâche. Mais cela ne signifie pas, pour autant, que la catastrophe soit systématiquement inévitable pour l'opérateur mis en service dans la même situation, d'où l'estimation à 10^{-1}/heure.

Ces deux estimations étant faites pour les deux classes extrêmes, les estimations pour les classes intermédiaires se font de façon arbitraire en supposant que le passage d'une classe à la classe de risque supérieur, multiplie par 100 la probabilité d'accident.

Ce raisonnement est valable pour les opérations rencontrées dans l'industrie et dans le transport. Il est à réviser pour les opérations spatiales, du moins tant que les astronautes ne travaillerons pas 2000 heures par an!

Dans ces conditions la probabilité d'accident au cours de la sous phase s'établit à partir du tableau :

CLASSE	PROBABILITÉ DE CLASSE P_{cl}	Probabilité Conditionnelle d'Accident par heure P_r	Probabilité d'Accident
A	P_A	10^{-11}	$\Pi_A = P_A \times 10^{-11}$
B	P_B	10^{-9}	$\Pi_B = P_B \times 10^{-9}$
C	P_C	10^{-7}	$\Pi_C = P_C \times 10^{-7}$
D	P_D	10^{-5}	$\Pi_D = P_D \times 10^{-5}$
E	P_E	10^{-3}	$\Pi_E = P_E \times 10^{-3}$
F	P_F	10^{-1}	$\Pi_F = P_F \times 10^{-1}$
			$P = \Sigma \Pi_I$

La probabilité d'accident Π_I calculée pour la classe I est le produit de la probabilité d'occurrence P_I de la classe I par la probabilité conditionnelle d'accident P_r affectée à cette classe. La probabilité d'accident P pour la sous phase est la somme des probabilités d'accidents Π_I de chaque classe.

A titre d'exemple supposons que nous ayons obtenu les résultats d'essai suivants :

CLASSE	TÂCHE	PROBABILITÉ DE TÂCHE	PROBABILITÉ DE CLASSE
A	a	$1-\alpha \# 1$	$1-\beta \# 1$
	c	10^{-5}	
	k	10^{-6}	
B	b	10^{-2}	$1,1 . 10^{-2}$
	e	10^{-3}	
	d	10^{-6}	
C	f	10^{-4}	$1,0 . 10^{-4}$
D	m	10^{-6}	$2,1 . 10^{-6}$
	g_{O1}	$1/3.10^{-6}$	
	g_{O2}	$1/3.10^{-6}$	
	g_{O3}	$1/3.10^{-6}$	
	i_{O3}	10^{-7}	
E	i_{O1}	10^{-7}	$3,2 . 10^{-7}$
	i_{O2}	10^{-7}	
	h h_1	10^{-8}	
	h h_i	10^{-8}	
	h h_{10}	10^{-8}	
	j_1	10^{-9}	
	j_2	10^{-9}	
F	j j_3	10^{-9}	$8,1 . 10^{-9}$
	j j_i	10^{-9}	
	j j_{10}	10^{-9}	
	l	10^{-10}	

La première colonne est consacrée aux classes de risque.

La deuxième colonne regroupe pour chaque classe toutes les tâches qui ont été jugées appartenant à la même classe de risque.
La probabilité P_t d'occurrence de chaque tâche figure dans la troisième colonne.
Enfin dans la dernière colonne figure la probabilité P_{Cl} de classe, qui est la somme des probabilités P_t des tâches de la classe.
Les valeurs choisies ne sont données qu'à titre d'exemples, permettant de mettre en lumière les cas particuliers rencontrés en pratique (on notera que le nombre de tâches est réduit; en général il en figure beaucoup plus pour une sous-phase donnée, si l'on tient compte de toutes les combinaisons de pannes et de conditions d'emploi).

- ⇨ Il est indispensable de dresser le tableau de l'ensemble des tâches sans en négliger aucune. Si l'on néglige par exemple les tâches j_3 à j_{10} sous prétexte que leur probabilité 10^{-9} est faible, on voit que l'on modifie substantiellement la probabilité de la classe F. Par contre la tâche d peut être négligée a posteriori sans que la probabilité de la classe B en soit modifiée.
- ⇨ La tâche h correspond par exemple à des conditions de freinage à un carré avec des visibilités comprises entre 500 et 1500 m. On pourrait décomposer cette tâche en dix "sous-tâches" h_1 à h_{10} pour des visibilités de 500, 600,..., 1400 et 1500 m (la probabilité de chaque sous tâche est le dixième de la probabilité de la tâche h). Si les dix sous-tâches sont regroupées dans la même classe de risque, ce "raffinement" ne change pas la probabilité de classe.

Par contre les tâches j_1 à j_{10} ne se plaçant pas dans la même classe, l'opérateur risquerait d'éprouver des difficultés d'estimation si on les regroupait en une seule tache j de probabilité 10^{-8}.

Cette remarque permet de définir la règle de découpage des tâches. Il est inutile de poursuivre la décomposition en sous-tâches si celles-ci se regroupent dans la même classe de risque.

⇨ Si l'on demande à plusieurs opérateurs d'évaluer le risque d'une même tâche, on peut rencontrer le cas d'évaluations divergentes.

Si ces évaluations sont très différentes, la même tâche étant classée par exemple en A par un opérateur et en F par un autre, il faut se poser le problème de la validité de l'expérimentation (mauvaise simulation des conditions d'emploi, mauvaise information des opérateurs, etc.) et rejeter les résultats tant que les différences n'ont pas été expliquées.

Par contre des faibles différences d'évaluation (écarts d'une classe) peuvent se produire. Ces résultats sont directement utilisables de la façon suivante.

Les tâches g et i ont été évaluées par trois opérateurs $\mathbf{O_1}$, $\mathbf{O_2}$, $\mathbf{O_3}$. Nous divisons artificiellement ces tâches en trois "sous-tâches", g_{O1}, g_{O2}, g_{O3}, i_{O1}, i_{O2}, i_{O3} et nous répartissons les probabilités P_g et P_i des tâches g et i entre les sous-tâches correspondantes. Cette répartition est arbitraire. Elle peut se faire de façon uniforme ou en accordant plus de poids à certains des opérateurs. Dans notre exemple c'est la répartition uniforme qui a été choisie ($P_g = 10^{-6}$ et $P_i = 3.10^{-7}$).

Les trois opérateurs ayant placé la tâche g dans la même classe D, la multiplication des opérateurs n'a pas changé le résultat.

Par contre l'opérateur O_3 a placé la tâche i en classe D et les deux autres en classe E. Il en résulte un léger changement pour la probabilité de la classe E et peu d'effet sur la probabilité de la classe D par rapport à une estimation reposant uniquement sur le jugement de l'opérateur O_1.

On notera que les classes ont été caractérisées par des lettres de A à F et non par des chiffres de 1 à 6 pour éviter la tentation d'interpréter des jugements de plusieurs opérateurs en faisant une opération de pondération sur les numéros de classe (la classe D,66 n'a pas de sens alors qu'il peut être tentant de parler de la classe 5,66 !).

On obtient alors résultat suivant:

CLASSE	PROBABILITÉ DE CLASSE P_{cl}	Probabilité Conditionnelle d'Accident par heure P_r	Probabilité d'Accident
A	1	10^{-11}	$1,0 . 10^{-11}$
B	$1,1 . 10^{-2}$	10^{-9}	$1,1 . 10^{-11}$
C	$1,0 . 10^{-4}$	10^{-7}	$1,0 . 10^{-11}$
D	$2,1 . 10^{-6}$	10^{-5}	$2,1 . 10^{-11}$
E	$3,2 . 10^{-7}$	10^{-3}	$32,0 . 10^{-11}$
F	$8,1 . 10^{-9}$	10^{-1}	$81,0 . 10^{-11}$
			$118,2 . 10^{-11}$

Il n'est pas question de donner une valeur absolue à ces résultats et d'en déduire par exemple que la probabilité d'accident au cours de la sous-phase étudiée est de $118,2.10^{-11}$, ni même de $1,2.10^{-9}$.

Cette méthode n'a pour objet que de comparer les poids relatifs des diverses tâches afin de ne pas négliger les cas qui pourraient apparaître a priori comme négligeables vis à vis de la sécurité, compte tenu de leur faible probabilité d'occurrence Pt.

On voit ainsi que les tâches classées E et F dans notre exemple (choisi aux fins de démonstration !) ont un poids important, malgré leurs probabilités d'occurrence que l'on pourrait juger faibles a priori. Il y aurait donc intérêt à modifier si possible ces probabilités d'occurrence, en jouant par exemple sur la fiabilité des systèmes en cause ou les conditions d'emploi.

Cette méthode permet également d'évaluer les poids relatifs des diverses sous-phases et de détecter a posteriori celles qui sont critiques et sur lesquelles il y a intérêt à porter un effort sur les plans fiabilité et conditions d'emploi.

Rappelons que les améliorations peuvent être apportées sur trois points :

⇨ Amélioration de l'"Opérabilité" du système en jouant, entre autres, sur :
- la présentation des informations
- la présentation des alarmes (en particulier hiérarchisation)
- la disposition et les modes d'action des commandes
- la réponse du système aux diverses commandes
- l'automatisation de certaines opérations de conduite
- révision des procédures
- révision des méthodes de formation et d'entraînement.

⇨ Amélioration de la fiabilité des systèmes en jouant, en autres, sur :
- la redondance des systèmes
- les conditions d'ambiance
- les règles d'utilisation
- les règles de maintenance

⇨ Modification des conditions d'emploi
par exemple,
interdiction d'effectuer certains travaux de nuit ou dans de mauvaises conditions météorologiques,
interdiction d'exécution d'une tâche en dehors d'un poste de travail déterminé, etc..

ANNEXE 4

VESTIBULE ET PILOTAGE

Lors des évolutions d'un avion, surtout d'un chasseur, le pilote se trouve soumis à des accélérations linéaires et angulaires et à des vitesses angulaires qui sont bien supérieures à celles rencontrées dans la vie courante.

Les capteurs humains qui détectent le mouvement ne sont pas adaptés aux circonstances ainsi rencontrées en vol et conduisent parfois le pilote à une mauvaise interprétation de la situation ce qui se traduit par un phénomène de désorientation appelé quelquefois, mais improprement, vertige ou à une fausse image de la situation le conduisant à une erreur de représentation.

Cette mauvaise interprétation de la situation est due aux imperfections des capteurs humains, seuil, précision, retard, imperfections qui sont sans effet notable dans la vie courante, mais qui ne sont plus négligeables lors des évolutions d'un avion. Par ailleurs des évolutions, en vol sans visibilité, peuvent également provoquer des troubles d'orientation du fait de la non corrélation des informations venant des divers capteurs.

Les différents capteurs jouant un rôle important dans la prise de conscience de l'orientation sont

- l'oreille interne qui détecte le sens et la grandeur des accélérations angulaires (et d'une façon plus ou moins nette le sens et la grandeur des vitesses angulaires) ainsi que la direction (mais non l'intensité) du vecteur facteur de charge,
- la vision centrale et la vision périphérique qui détectent les positions et les vitesses angulaires,
- les parties du corps en contact avec les surfaces d'appui qui détectent l'intensité et la direction des forces de contact, forces en relation directe avec la grandeur et la direction du vecteur facteur de charge subi par le pilote.

Nous ne cherchons pas dans ce court exposé à identifier les capteurs responsables des divers troubles rencontrés en vol. Néanmoins, dans un simple souci de classement, nous regrouperons les différents troubles en cherchant à les attribuer à des défauts d'un même capteur, mais seul le bon sens et non la rigueur scientifique nous servira de guide.

I - TROUBLES DUS AUX CAPTEURS DE GRAVITE

Par capteurs de gravité, nous entendons ici tous les capteurs, oreille interne ou surfaces du corps, capables de fournir des informations sur l'intensité et la direction des facteurs de charge subis par le pilote.

Ces capteurs ne sont pas plus capables que les accéléromètres placés à bord de l'avion de détecter la direction des forces de gravité, hormis le cas du déplacement rectiligne uniforme. Ils ne fournissent que la direction de la verticale apparente, c'est-à-dire la direction du vecteur facteur de charge.

Rappelons qu'un accéléromètre linéaire mesure le facteur de charge (et non l'accélération au point de mesure). Le vecteur facteur de charge est égal (si le véhicule ne tourne pas autour de son centre de gravité ou si l'accéléromètre est placé au centre de gravité) à la résultante de toutes les forces appliquées au véhicule, excepté le poids du véhicule, divisée par la valeur (scalaire) du poids du véhicule. Autrement dit il mesure la différence vectorielle $\boldsymbol{\Gamma} - \mathbf{g}$ entre le vecteur accélération $\boldsymbol{\Gamma}$ du véhicule et le vecteur accélération $\mathbf{g}$ de la pesanteur (voir Complément 1 en fin d'annexe).

C'est ainsi qu'au cours d'un palier accéléré le pilote aura la sensation de voler en montée et qu'au cours d'un palier décéléré il aura la sensation de voler en descente.

Il est bien évident que sur un véhicule terrestre ou marin, les sensations seront les mêmes, mais avec deux différences très importantes :

- les niveaux d'accélérations usuels y sont beaucoup plus faibles,
- le pilote sait que son véhicule reste sur le sol et il traduit instinctivement la sensation en terme d'accélération et non en terme de pente s'il sait que le véhicule se déplace horizontalement.

Un avion de chasse, fortement motorisé peut avoir au décollage une accélération horizontale voisine de l'accélération de la pesanteur ce qui conduit à la sensation de montée avec une pente de 45°. Un avion de transport du type Concorde a, au lâcher des freins, une accélération de l'ordre de 0,4 fois l'accélération de la pesanteur, ce qui donne une sensation de montée sous un angle de 20° environ.

Ce type de désorientation est en général peu dangereux, dans la mesure où la vision du monde extérieur et en particulier de l'horizon, permet au pilote de se "recaler". Néanmoins, certains accidents au décollage peuvent lui être imputés lorsque les circonstances, décollage de nuit avec mauvaise visibilité, pannes de systèmes (moteur en particulier) absorbant une partie de l'attention du pilote, ont amené celui-ci à pousser sur le manche, une fois l'avion décollé, pour réduire, de façon réflexe, une pente de montée ressentie comme excessive.

Les capteurs de gravité sont par ailleurs peu précis. Lorsque les références visuelles sont mauvaises, ils ne permettent pas de reconnaître la verticale avec une précision suffisante, même en vol à vitesse uniforme (donc sans effet de verticale apparente). C'est ainsi qu'un pilote peut prendre pour horizon, un faux horizon décalé de quelques degrés vers le haut ou vers le bas (banc de brume, ligne de nuages en particulier sur horizon marin). Cette erreur est en général sans conséquence, sauf en cas de vol à basse altitude, où le pilote peut découvrir très tardivement que telle ligne de crête est à une altitude supérieure à celle estimée par comparaison avec un faux horizon.

L'incident suivant qui n'a d'ailleurs qu'un intérêt anecdotique montre bien que l'appréciation de la verticale (ou de l'horizontale) se fait avec une imprécision excessive. Un terrain d'Afrique possédait une ligne de balises d'entrée de piste, qui installée parallèlement au sol, se trouvait inclinée de quelques degrés sur l'horizontale; l'expérience a montré que les pilotes non avertis avaient tendance, au cours de l'approche, à mettre le "plan des ailes" parallèle à la ligne de balises dès que cette ligne était vue sous un angle suffisamment grand pour pouvoir fournir une référence. L'avion ainsi mis en léger virage sortait de l'axe d'approche et il fallait un temps non négligeable au pilote pour reconnaître la situation et revenir à la référence donnée par l'horizon artificiel pour effectuer la manœuvre de correction.

II - TROUBLES DUS AUX CAPTEURS D'ACCELERATION ANGULAIRE

Les canaux semi-circulaires ne détectent les accélérations angulaires qu'au-delà d'un certain seuil et par ailleurs une mise en rotation suivie d'une rotation à vitesse angulaire constante se traduit au bout de quelques dizaines de secondes par une suppression de toute sensation de rotation ; lors de l'arrêt de cette rotation, le sujet a la sensation d'accélération angulaire puis de rotation constante en sens inverse (voir Complément 2).

Ces deux types d'imperfections sont sans doute à l'origine d'un trouble bien connu des pilotes se traduisant, en vol sans visibilité, par la sensation de virage continu (avec une forte inclinaison latérale) alors que les instruments, en particulier l'horizon, montrent que le vol est parfaitement rectiligne.

Il est difficile de préciser si cette sensation erronée est due à l'effet de seuil (mise en virage lente non détectée suivie d'un retour rapide au vol rectiligne) ou à l'effet d'hystérésis du capteur (retour au vol rectiligne après un vol en virage prolongé). Suivant les cas, il est probable que l'une ou l'autre des deux imperfections de l'oreille interne est la cause du trouble. Presque tous les pilotes ont rencontré, au moins une fois, ce type de désorientation en vol sans visibilité; c'est un phénomène extrêmement désagréable car il oblige le pilote à maintenir son attention de façon quasiment permanente sur l'horizon artificiel pour ne pas céder au réflexe qui le pousse à agir sur le manche en gauchissement pour "corriger" le virage dès qu'il surveille un autre paramètre (altitude, vitesse, pente, navigation, échange radio avec le contrôle au sol, etc.).

Il est tout aussi difficile de préciser quelles sont les circonstances favorisant l'apparition de ce type de désorientation. Il apparaît toutefois que l'absence totale de la vision extérieure (vol de nuit dans la brume, vol d'entraînement sous capote), le vol en patrouille avec un mauvais horizon (le pilote, l'œil fixé sur le leader, ne recueille plus d'information visuelle sur sa position par rapport à l'horizon si celui-ci n'est pas très net), une charge de travail élevée (qui augmente les seuils de perception minimale), un mauvais état physique et mental (légère congestion des sinus, usage de drogues agissant sur la circulation du sang, anxiété, etc.), favorisent l'apparition de ces troubles. Il faut noter qu'en vol dans les nuages de jour, la vision périphérique détecte, non pas l'assiette latérale, mais les variations d'assiette latérale. En général en effet les nuages ne sont pas très homogènes (variation de teintes, paquets plus ou moins denses, etc.), et la lumière du soleil bien que diffuse, donne une direction de référence. Par contre en vol de brume sous une couverture nuageuse importante de jour ou en vol de nuage de nuit, la vision périphérique ne détecte plus rien.

D'un autre côté, il semble qu'une forte turbulence ne favorise pas l'apparition du phénomène, peut-être parce que les agitations de l'avion dépassent en permanence les seuils de perception.

Un remède quelquefois recommandé consiste à effectuer des balancements latéraux, soigneusement suivis à l'horizon artificiel, ce qui permettrait de "recaler le capteur d'accélération angulaire au zéro" !

III - EFFET DE CORIOLIS SUR LES CANAUX SEMI-CIRCULAIRES

On sait que si un mobile se déplace avec une vitesse **V** par rapport à un système de référence lui-même animé d'un mouvement de rotation **Ω** par rapport à un système de référence absolu, le mobile est soumis à une accélération $\mathbf{\Gamma} = 2 . \mathbf{\Omega} \wedge \mathbf{V}$ ($\wedge$ représente le produit vectoriel; ainsi le vecteur **Γ** est-il normal au plan contenant **Ω** et **V** et son module est égal au produit des modules de **Ω** et de **V** et du sinus de l'angle entre **Ω** et **V;** ce module est donc maximal si **Ω** et **V** sont rectangulaires et nul s'ils sont parallèles.).

Le liquide contenu dans les canaux semi-circulaires est soumis à cette accélération ce qui peut créer une sensation parasite de rotation lorsque le pilote bouge la tête alors que l'avion est en évolution.

Cette sensation est maximale lorsque la rotation de la tête se fait autour d'un axe perpendiculaire à l'axe de rotation de l'avion et l'effet est ressenti comme une rotation autour de la perpendiculaire commune à l'axe de rotation avion et à l'axe de rotation de la tête.

Ainsi le fait de baisser la tête (axe de rotation de la tête horizontal gauche-droite) au cours d'un virage en palier (axe de rotation de l'avion vertical) se traduira par une sensation de rotation en roulis (balancement gauche - droite ou droite - gauche). Au cours du même virage, le fait de pencher la tête latéralement (axe de rotation de la tête horizontal avant-arrière), se traduira par une sensation de rotation de tangage (à cabrer ou à piquer).

Au cours d'une ressource, le fait de tourner la tête (autour d'un axe vertical) pour regarder sur le côté, se traduira par une sensation de roulis ; le fait d'incliner latéralement la tête se traduira par une sensation de lacet (rotation autour d'un axe vertical).

Au cours d'un tonneau (rotation de l'avion autour d'un axe parallèle à la vitesse), le fait de baisser la tête se traduira par une sensation de lacet et le fait de tourner la tête pour regarder sur le côté, par une sensation de mouvement de tangage.

On peut démontrer que la rotation d'un angle θ pendant le temps T autour d'un axe perpendiculaire à l'axe de rotation avion (vitesse de rotation **Ω**), se traduit par une sensation identique à celle que produirait la mise en rotation pendant le même temps T sur le troisième axe jusqu'à une vitesse angulaire :

$$\omega = \mathbf{\Omega} . \sin \theta$$

Autrement dit, si au cours d'un virage horizontal le pilote baisse la tête en la faisant tourner de 90° (pour passer de la position œil fixé au-dessus de l'horizon à la position œil sur une banquette latérale pour changer par exemple une fréquence radio; $\theta = 90$ et $\sin \theta = 1$), ce mouvement se traduira par une sensation de mise en roulis jusqu'à une vitesse de rotation égale à la vitesse de rotation de l'avion.

Ainsi au cours d'une approche à la vitesse de 120 kt (60 m/s) en virage incliné à 30°, la vitesse de changement de cap est de 5,5 degrés par seconde. Le pilote aura donc l'impression en baissant la tête que l'avion est animé d'une vitesse de roulis de 5,5 degrés par seconde ce qui ne va pas manquer de lui faire contrer cette rotation apparente par un coup de manche en roulis.

Ce phénomène est sans doute à l'origine de quelques accidents survenus en approche sur des avions de chasse où le pilote devait en dernier virage effectuer un changement de fréquence radio en manipulant un contacteur placé très en arrière sur la banquette gauche, ce qui l'obligeait à baisser fortement la tête pour le repérer visuellement; on a pu observer au cours de cette phase de vol des passages de l'avion sur le dos dus sans doute à une manœuvre instinctive du pilote contrant une sensation erronée de rotation lui faisant croire que l'avion revenait "ailes horizontales" (un changement de procédure n'imposant plus le changement de fréquence a été décidé et les accidents ont cessé, mais il est difficile de conclure quant à la véracité de l'explication).

IV - FACTEURS AGGRAVANT LA DESORIENTATION

De l'avis de nombreux pilotes et à la suite d'expérimentations systématiques effectuées en particulier par la NASA, il ressort que les phénomènes de désorientation apparaissent préférentiellement lors de manœuvres effectuées au moment du passage des conditions de vol à vue aux conditions de vol aux instruments.

L'expérience montre qu'il faut environ 30 secondes à un pilote pour analyser la situation lors d'un passage vol à vue, vol aux instruments.

Ce temps nécessaire au pilote pour s'habituer aux nouvelles références fournies par les instruments de bord a été mesuré en demandant à des pilotes d'effectuer une manœuvre très simple de changement de cap (30° de changement de cap à un taux de 3°/s) dès que possible après une mise sous capote à un moment non prévu. Il s'agit ici de tableaux de bord conventionnels non équipés de viseurs tête haute qui fournissent des informations beaucoup plus proches de celles recueillies en vol à vue.

Ceci montre combien peut être dangereux d'effectuer des manœuvres comportant un risque de désorientation au moment du passage vol à vue, vol aux instruments. Aussi est-il recommandé au pilote de passer volontairement au vol aux instruments avant de pénétrer dans la couche de façon à s'habituer aux références nouvelles fournies par les instruments, alors que les informations de positions angulaires fournies par la vision périphérique sont encore disponibles. Il est également recommandé de ne pas effectuer, si possible, de manœuvres dans les 30 secondes suivant le passage aux instruments.

Nous venons de montrer que les informations de position angulaire de l'avion, fournies par la vision périphérique, étaient très utiles au pilotage ; leur absence en vol aux instruments favorise la désorientation.

Il faut noter que la sensation de virage permanent, alors que l'avion vole en ligne droite n'est en rien supprimée par l'observation de l'horizon artificiel : c'est un processus intellectuel "douloureux" qui persuade le pilote que ses sensations sont fausses sans pour autant les éliminer. Par contre cette sensation cesse instantanément dès le passage en vol à vue.

Les références visuelles sont indispensables au pilotage. La lecture de l'horizon artificiel ou des instruments pouvant fournir des indications d'attitude, ou celle des autres instruments (altimètre, variomètre, indicateur de cap, bille et aiguille) est moins commode que la vue du monde extérieur, mais elle est indispensable. Toute tentative de pilotage les yeux fermés se traduit par une perte de contrôle au bout d'un temps n'excédant pas deux minutes. Cette remarque peut sembler académique ; que l'on se souvienne toutefois qu'un éclair de nuit, peut aveugler un pilote pendant un temps non négligeable, d'où la nécessité en orage d'aveugler les fenêtres de la cabine de pilotage et d'éclairer au maximum le tableau de bord pour limiter le temps d'éblouissement.

Nous venons de voir que la difficulté de pilotage rencontrée au moment du passage au vol aux instruments venait essentiellement de la perte d'informations provenant de la vision périphérique. L'expérience suivante que nous avons maintes fois effectuée le démontre aisément. Au cours d'approche ILS ou GCA* en conditions réelles de vol aux instruments (nuages de nuit ou vol sous capote) les ailes ne sont maintenues "horizontales", surtout par temps turbulent, que par surveillance serrée de l'horizon artificiel (en pratique, il est conseillé d'effectuer une lecture de l'horizon après tout autre instrument, altimètre, cap, vitesse, indicateur d'ILS, etc.). Si par contre, on effectue une approche avec les mêmes conditions de turbulence sans capote mais siège en position basse en s'astreignant à ne pas regarder à l'extérieur et à regarder uniquement les instruments, les ailes restent, semble-t-il miraculeusement, "horizontales" ; dans ce cas en effet, la vision périphérique capte, sans que le pilote en ait conscience, les changements d'assiette latérale qui sont aussitôt corrigés en agissant sur le gauchissement par acte purement réflexe.

Ainsi l'absence de références visuelles (surtout en provenance de la vision périphérique) favorise la désorientation. Ce phénomène peut par ailleurs être aggravé lorsque les informations en provenance de l'oreille interne sont en contradiction avec les informations provenant de l'œil : effectuer un virage à inclinaison latérale variable en regardant l'aile haute sur fond de ciel pur (pas de vision du mouvement) se traduit très rapidement par un malaise. Voler aux instruments avec un horizon artificiel en panne conduit aussi rapidement au malaise car les informations fausses fournies par l'instrument et collectées involontairement par l'œil sont en contradictions avec le mouvement réel de l'avion ressenti par l'oreille interne (en général ce phénomène est évité en masquant par un cache l'horizon défaillant).

Deux exemples vont illustrer le problème de la non corrélation des informations en provenance de l'oreille interne (et des capteurs des réactions d'appui du corps sur le siège) et en provenance de la vision périphérique.

Nous avons tous remarqué qu'il est très pénible de suivre sur un écran de télévision et encore plus sur un écran large de cinéma, les images prises à bord d'un véhicule en évolution. Nous éprouvons très rapidement le besoin de quitter les images des yeux car nous ne ressentons pas les accélérations qui devraient accompagner les images. Cet effet avait d'ailleurs été abondamment exploité dans les premiers films tournés en cinérama.

Au cours de la mise au point du mouvement cabine d'un simulateur de vol, une erreur de programmation avait conduit à ce que la cabine réponde à l'envers aux sollicitations du manche en gauchissement, alors que l'horizon artificiel répondait correctement. L'opérateur qui n'avait pas de vue sur le monde extérieur se référait aux

mouvements de l'horizon artificiel, correctement corrélés à ses commandes, mais ressentait, sans en avoir conscience, des mouvements de rotation en sens inverse. Cette situation l'a très rapidement conduit au malaise (c'était un pilote de chasse confirmé !) et il a fallu un certain temps avant de découvrir l'origine de ces troubles.

Le malaise lié à la non corrélation entre les informations en provenance de l'œil et de l'oreille interne est en partie dû au fait que l'oreille interne "pilote" l'œil pour le maintenir fixe par rapport au monde extérieur. Ce dernier phénomène a une conséquence importante; lorsque l'avion est soumis à des turbulences, l'œil maintenu, si la turbulence n'est pas trop intense, en position angulaire fixe par rapport au monde extérieur, est en mesure de capter aisément les informations en provenance de ce monde extérieur (horizon réel, position de la piste d'atterrissage) mais éprouve beaucoup de difficultés à recueillir les informations des instruments de bord. Cette remarque milite en faveur de la présentation d'informations liées au monde extérieur, collimatées à l'infini, sur des viseurs tête haute.

Pour résumer les conditions qui favorisent l'apparition de phénomènes de désorientation, nous citerons :

- les conditions de vol :
    - visibilité réduite,
    - turbulence,
    - vol de nuit (au décollage en particulier),
    - vol en patrouille, ravitaillement en vol par mauvaise visibilité,
    - passage du vol à vue au vol aux instruments.

- le comportement du pilote :
    - mouvements de la tête en évolution (lecture de carte, changement de fréquence radio, réglage altimétrique, manipulation d'interrupteurs de commande du système d'arme, de boutons de réglage du radar, etc.),
    - tentative de vol à vue par mauvaise visibilité (surtout par passages intermittents dans les nuages).
    - les manœuvres :
        - virage prolongé avec retour rapide au vol rectiligne (montée spirale et mise en palier rectiligne),
        - mise en virage lente,
        - accélération et décélération brutales,
        - passage au vol aux instruments au cours de manœuvres acrobatiques,
        - variations importantes et rapides d'altitude (le non équilibrage des pressions de part et d'autre de l'oreille moyenne peut conduire à des troubles de l'équilibre).
    - l'inexpérience et le faible entraînement au vol aux instruments : l'expérience conduit les pilotes à se méfier des informations fournies par ses propres capteurs de gravité et à ne se fier qu'aux informations visuelles fournies par les instruments.
    - l'état physique et mental du pilote : une sinusite même légère et un état d'anxiété sont très favorables à l'apparition de troubles d'orientation.

Parmi tous ces facteurs, nous retiendrons les plus "actifs" :

- la faible expérience et le manque d'entraînement,
- les changements de position de la tête en manœuvre,
- le changement de références en vol (vol à vue / vol aux instruments, vol en patrouille / vol aux instruments, mélange de deux modes de pilotage),
- l'anxiété.

V - LES REMÈDES À LA DÉSORIENTATION

On ne peut modifier les capteurs humains. Il faut se rendre à l'évidence, l'homme n'est pas fait pour voler. C'est ce dont tout pilote prend conscience lorsqu'il se trouve de nuit dans un beau "cunimb" (un cumulo-nimbus d'orage), secoué par les rafales, aveuglé par les éclairs et assourdi par le tintamarre des grêlons sur le pare-brise!

On ne peut donc, à proprement parler, faire état de remèdes à la désorientation ; peut-on tout au plus chercher à limiter les facteurs favorisant l'apparition du phénomène.

Il faut entraîner les pilotes de façon à les habituer à ignorer les "sensations" en vol aux instruments (c'est ce que les pilotes appellent "ne pas voler aux fesses", mais aux instruments).

L'entraînement permet également aux pilotes de reconnaître l'existence de ces phénomènes de désorientation dans des conditions, où sentant leur sécurité assurée par le moniteur, ils n'en subissent que les effets physiologiques et non psychologiques, ce qui leur évitera l'anxiété en opération réelle; l'entraînement peut ainsi aider à reconnaître le phénomène et à le combattre.

Par ailleurs, l'application de procédures strictes de pilotage peut limiter l'apparition du phénomène :

- ne pas concentrer son attention sur un seul instrument (vérification croisée de la situation par balayage de tous les instruments de façon à améliorer l'évaluation de la situation de l'avion en oubliant les sensations),
- ne pas bouger la tête, en vol aux instruments, ou du moins éviter les mouvements rapides de grande amplitude,
- en cas de désorientation passer les commandes au copilote. Sur monoplace, essayer de se détendre et effectuer des manœuvres amples de roulis contrôlées à l'horizon artificiel,
- ne pas tenter de faire du pilotage "mixte" en mélangeant les références du vol à vue et du vol aux instruments,
- passer au vol aux instruments, si possible, trente secondes au moins avant de pénétrer dans la couche,
- rester si possible en vol rectiligne entre 30 et 45 secondes après passage au vol aux instruments.

VI - CONCLUSIONS

Ce court exposé n'était pas destiné à faire le tour de la question des phénomènes de désorientation en vol. Il n'a traité que quelques cas rencontrés le plus fréquemment et relativement bien identifiés. Ils sont dus, le plus souvent à une non corrélation entre les informations assez pauvres fournies par l'observation visuelle des instruments de bord classiques et les sensations fournies généralement par le système vestibulaire, système que le hasard et la nécessité n'ont pas encore eu le temps de faire évoluer chez l'"homo-volans".

ANNEXE 4

COMPLEMENT 1

Facteur de Charge. Verticale apparente

Plaçons un pendule, constitué d'une bille tenue par un fil sans masse, au centre d'inertie **G** de l'avion en vol.

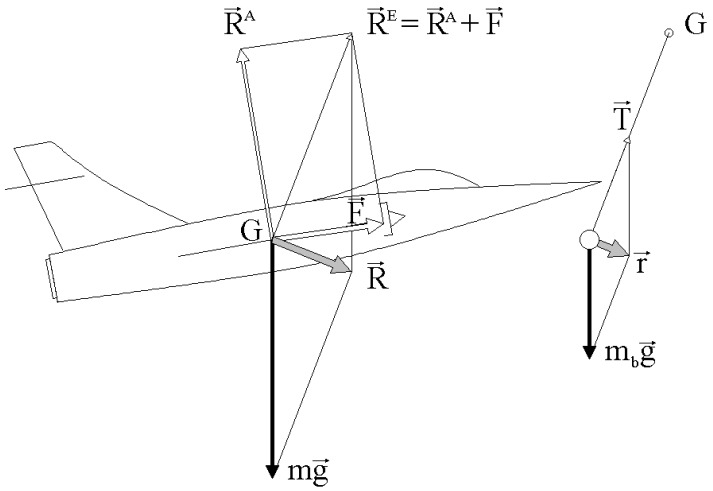
L'avion est soumis,

- aux forces aérodynamiques dont la résultante au centre d'inertie est $\mathbf{R}^A$,
- aux forces de propulsion dont la résultante au centre d'inertie est **F**,
- aux forces de gravité dont la résultante au centre d'inertie est le poids m**g**. (**g** est l'accélération de la pesanteur, m la masse de l'avion)

L'accélération $\mathbf{\Gamma}_a$ du centre d'inertie est égale à **R**/m, où **R** est la somme géométrique de ces trois résultantes (Théorème du mouvement du centre d'inertie).

La bille du pendule est soumise,

- à la traction **T** du fil
- aux forces de gravité dont la résultante au centre d'inertie de la bille est son poids $m_b\mathbf{g}$. (m_b est la masse de la bille)



L'accélération $\mathbf{\Gamma}_b$ du centre d'inertie de la bille est égale à **r**/m, où **r** est la somme géométrique de **T** et de $m_b\mathbf{g}$.

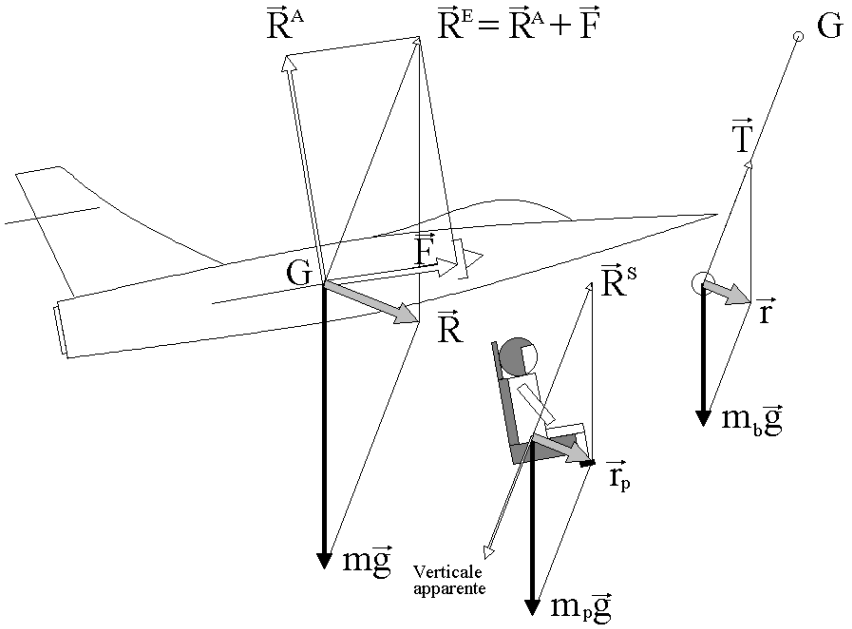
Le pendule étant supposé en équilibre par rapport à l'avion, l'accélération $\mathbf{\Gamma}_b$ de la bille est égale à l'accélération $\mathbf{\Gamma}_a$ de l'avion.

La comparaison des deux diagrammes de forces montre alors que **r** et **R** d'une part, m**g** et $m_b\mathbf{g}$ d'autre part, étant parallèles et dans le rapport de m à m_b, les forces **T** et $\mathbf{R}^E$ (somme de $\mathbf{R}^A$ et **F**) sont parallèles et dans le même rapport de m à m_b.

Ainsi un pendule s'oriente dans la direction de la somme de toutes les forces appliquées à l'avion (sauf les forces de gravité) et la force de traction du fil est égale à cette somme multipliée par le rapport m_b/m.

La mesure de la force **T** permet ainsi de connaître la force $\mathbf{R}^E$. En pratique on mesure la force **T** (par l'élongation d'un ressort par exemple) et donc n = $\mathbf{T}/m_b g$, qui est égal à $\mathbf{R}^E$/mg. La valeur de n est l'intensité du **vecteur facteur de charge** dont la direction est celle du fil (donc de $\mathbf{R}^E$).

Nous supposerons que l'avion ne tourne pas autour de son centre d'inertie.
Le pilote sur son siège est soumis,
- aux forces de contact du siège dont la résultante est $\mathbf{R}^S$
- aux forces de gravité dont la résultante au centre d'inertie du pilote est son poids $m_p\mathbf{g}$. (m_p est la masse du pilote).

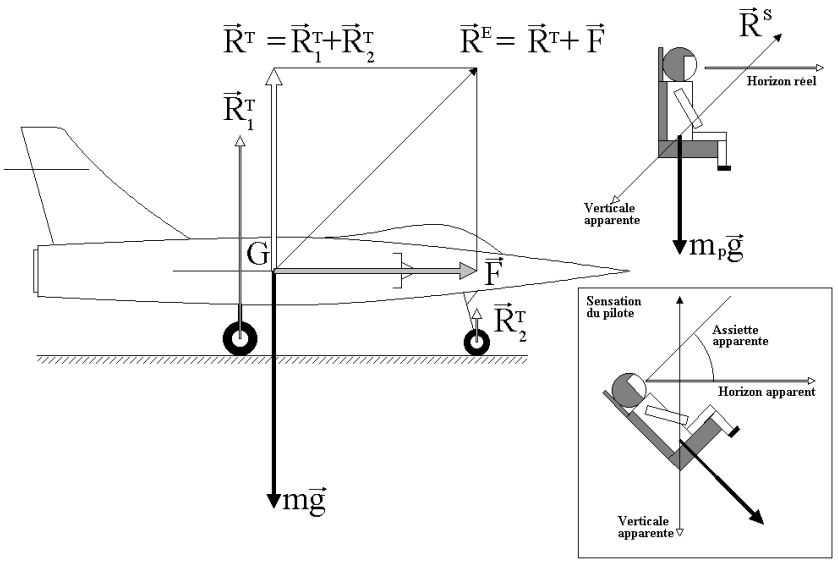


L'accélération $\mathbf{\Gamma}_p$ du centre d'inertie du pilote est égale à $\mathbf{r}_p/m$, où $\mathbf{r}_p$ est la somme géométrique de $\mathbf{R}^S$ et de $m_p\mathbf{g}$. Le pilote étant fixe par rapport à l'avion (heureusement !), et l'avion ne tournant pas autour du centre d'inertie, $\mathbf{\Gamma}_p$ est égal à $\mathbf{\Gamma}_a$.

La comparaison des trois diagrammes de forces montre alors que les forces $\mathbf{r}$, $\mathbf{R}$ et $\mathbf{r}_p$, d'une part, $m\mathbf{g}$, $m_b\mathbf{g}$ et $m_p\mathbf{g}$. d'autre part, étant parallèles et proportionnelles à m, m_b et m_p les forces $\mathbf{T}$, $\mathbf{R}^E$ et $\mathbf{R}^S$ sont parallèles et proportionnelles à m, m_b et m_p.

$$\mathbf{R}^S = n.\, m_p.\mathbf{g}$$

Ainsi la réaction $\mathbf{R}^S$ du siège sur le pilote est-elle proportionnelle à son poids et au facteur de charge n. Les sensations du pilote sont celles qu'il aurait si la verticale avait tourné pour être parallèle à la résultante $\mathbf{R}^E$ et si l'accélération de la pesanteur avait été multipliée par n.

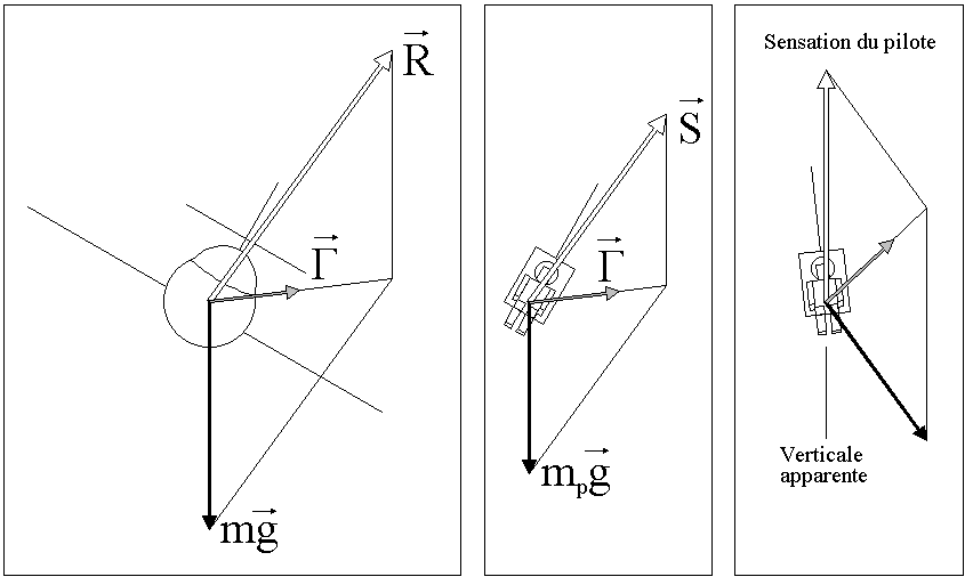


Dans le cas d'un décollage, où la poussée des moteurs serait égale au poids de l'avion, celui-ci, au lâcher des freins, est soumis (la vitesse est nulle, les forces aérodynamiques sont nulles),

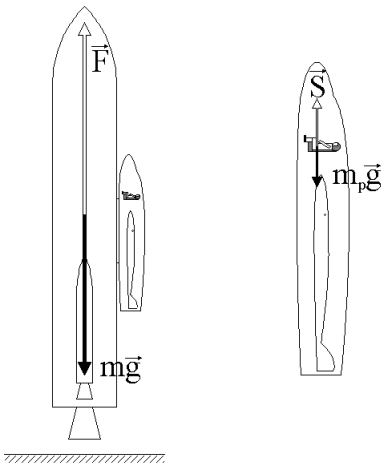
- aux forces de réaction du sol sur le train d'atterrissage, dont la résultante est $\mathbf{R}^T$ (verticale, équilibrant le poids $m\mathbf{g}$ de l'avion),
- aux forces de propulsion dont la résultante est $\mathbf{F}$ (horizontale et supposée de module égal à mg),
- aux forces de gravité dont la résultante est le poids $m\mathbf{g}$.

La résultante $\mathbf{R}^E$ de la poussée $\mathbf{F}$ et de la réaction $\mathbf{R}^T$ du sol est alors inclinée à 45 degrés sur l'horizontale.
Pour le pilote, tout se passe comme si la pesanteur avait tourné de 45 degrés et était multipliée par 1,4 (racine de 2).

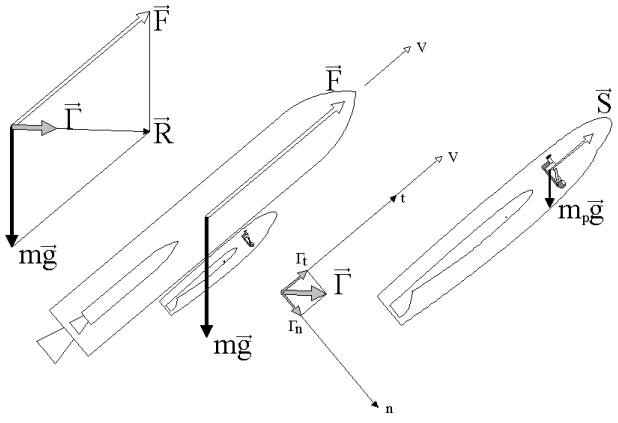
Dans le cas d'un virage dérapé (la résultante **R** des forces aérodynamiques n'est pas dans le plan de symétrie de l'avion du fait du dérapage), le pilote a l'impression que la verticale est parallèle à la force **R** et donc que l'avion "penche à droite", alors qu'il est incliné à gauche (avion vu de face sur la figure).



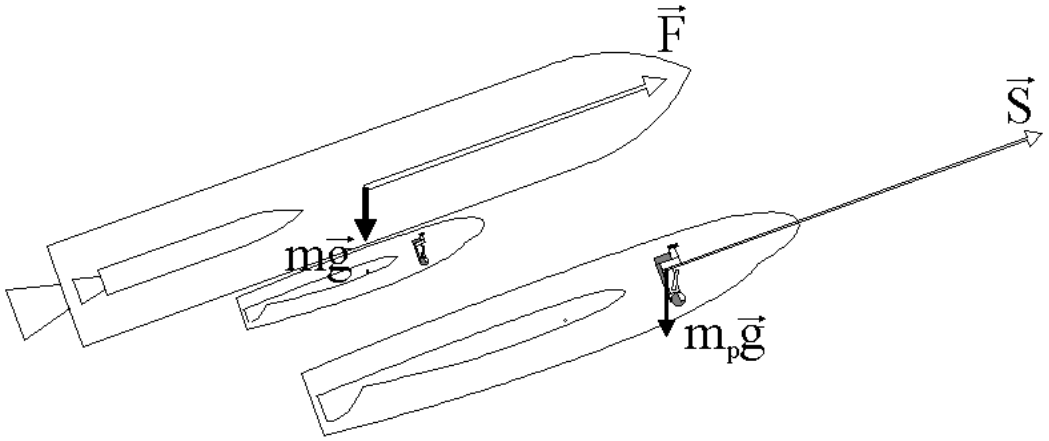
Examinons maintenant le décollage de la navette montée sur son lanceur. La poussée des moteurs est supposée égale à 1,2 fois le poids de l'ensemble lanceur + navette. Le vecteur facteur de charge a un module égal à 1,2 et est orienté suivant la poussée **F**, donc suivant l'axe du lanceur. Le lanceur est soumis à la force **F** et à son poids m**g**, donc à une résultante verticale de module F - mg. L'accélération est donc verticale et de module (F - mg) / m = 0,2g soit 2 m/s^2. Le pilote est soumis à une réaction **S** du siège parallèle au vecteur facteur de charge, donc verticale, égale à 1,2 fois son poids $m_p g$. Il a la sensation que l'accélération de la pesanteur a été multipliée par 1,2.



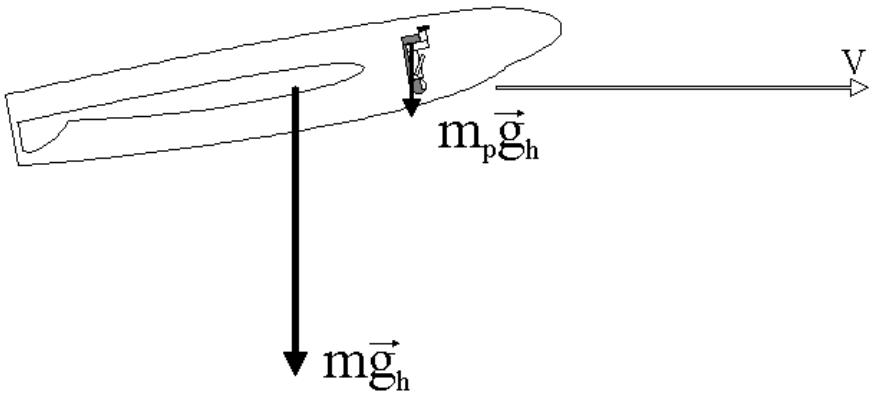
La navette et son lanceur sont maintenant en altitude avec une assiette de 50°. La masse lanceur + navette n'est plus que 80% de la masse au décollage et la poussée des moteurs est inchangée. Le vecteur facteur de charge, toujours parallèle à la force de poussée **F,** a maintenant un module égal à 1,5. La résultante **R** de la poussée **F** et du poids m**g** n'est plus verticale. Il en résulte une accélération **Γ** dont la composante Γ_t sur le vecteur vitesse (égale à dV/dt) augmente la vitesse et la composante normale Γ_n courbe la trajectoire vers le bas (le rayon de courbure *R* est donné par $R = V^2/\Gamma_n$). La réaction **S** du siège sur le pilote est parallèle au vecteur facteur de charge, donc parallèle à l'axe du lanceur et égale à 1,5 fois le poids $m_p g$. Le pilote a la sensation d'être toujours dans la même position par rapport à la terre et de subir une pesanteur multipliée par 1,5.



Lorsque la masse lanceur + navette n'est plus que 20% de la masse au décollage (fin de combustion, l'assiette est de 20°), le facteur de charge, toujours parallèle à la poussée, a un module égal à 6. La réaction du siège sur le pilote est parallèle à l'axe du lanceur et vaut 6 fois le poids $m_p g$. Le pilote a encore la sensation d'être toujours dans la même position par rapport à la terre et de subir une pesanteur multipliée par 6.



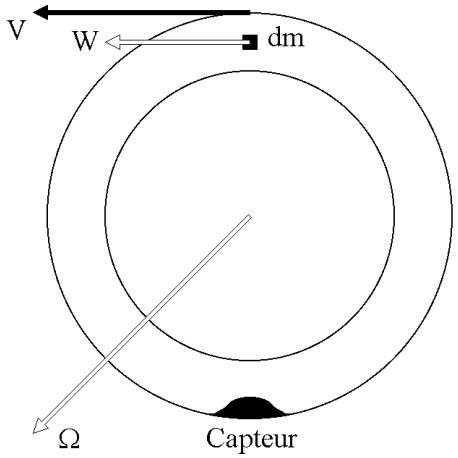
Enfin la navette est en orbite à 300 km, moteur éteint. Elle est soumise à son seul poids $m\mathbf{g}_h$($\mathbf{g}_h$ est l'accélération de la pesanteur à 300 km soit environ 8,94 m/s^2). Son accélération est donc verticale et égale à $\mathbf{g}_h$. Si sa vitesse est horizontale et voisine de 7700 m/s, le rayon de courbure de la trajectoire est $R = V^2/ g_h$ = 6.366.000 (rayon de la terre) + 300.000 m. La navette décrit une trajectoire circulaire à l'altitude constante de 300 km. Le vecteur facteur de charge est nul puisque la seule force agissant sur la navette est son poids. Il en résulte que la réaction du siège sur le pilote est nulle. Le pilote "flotte" dans la navette. Il est en état d'impesanteur. On remarquera qu'il est toujours soumis à son poids $m_p\mathbf{g}_h$ (son accélération est donc égale à $\mathbf{g}_h$ comme pour la navette). Ceci explique le terme *impesanteur* utilisé plutôt qu'*apesanteur* qui signifie absence de pesanteur, ce qui n'est pas le cas.



COMPLEMENT 2

L'oreille interne

L'un des trois canaux semi-circulaires composant en partie l'oreille interne peut être schématisé comme indiqué sur la figure ci-dessous.



Lors d'un mouvement de rotation autour d'un axe perpendiculaire au plan du canal, le liquide lymphatique, situé à l'intérieur du canal, a tendance, par inertie à rester fixe par rapport à un repère lié à la terre. Il est entraîné par effet de viscosité par la paroi du canal. Le mouvement du liquide qui en résulte est détecté par la déformation d'une masse gélatineuse à la base de laquelle parviennent les nerfs. Cette masse est en équilibre hydrostatique, ce qui la rend insensible aux accélérations linéaires. Nous supposerons que le signal envoyé au cerveau est fonction de la déformation de la masse gélatineuse donc des forces hydrodynamiques sur cette masse. En conséquence le signal est fonction de la vitesse d'écoulement du liquide lymphatique par rapport à la paroi.

Soit **V** la vitesse linéaire de la paroi suite à une rotation **Ω** et **W** la vitesse linéaire d'une particule de masse dm du liquide lymphatique. **V** et **W** sont des vitesses absolues dans un repère lié à la terre.

La force s'exerçant sur la particule, due à la viscosité du liquide, est proportionnelle à la vitesse de la particule par rapport à la paroi, soit **V - W**. Il en résulte une accélération **dW/dt** donnée par

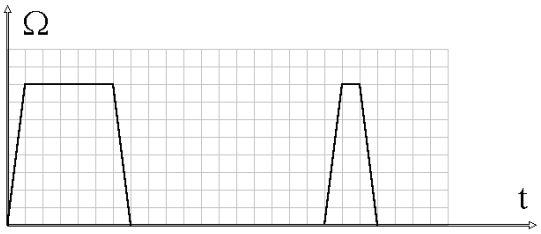
$$\mathbf{dW/dt = k . (V - W)}$$

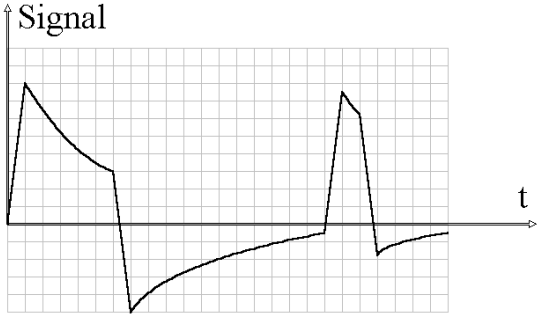
Le capteur détecte la vitesse **U = V - W** du liquide par rapport à la paroi; l'équation régissant **U** et par suite le signal envoyé au cerveau, que nous assimilons à U, s'écrit alors:

$$\mathbf{dU/dt + k . U = dV/dt}$$

V étant proportionnel à la vitesse de rotation **Ω** (**V** = λ.**Ω**) , la relation entre le signal **U** et la vitesse de rotation **Ω** est :

$$\mathbf{dU/dt + k . U = \lambda . d\Omega/dt}$$





Cette équation, une fois intégrée, donne la relation, signal **U**, vitesse de rotation **Ω**, pour une variation linéaire **Ω** = a + b . t

$$\mathbf{U = U_0\ e^{-k\,.\,(t - t_0)} + \mu\,.\,(1 - e^{-k\,.\,(t - t_0)})}$$

où $\mathbf{U_0}$ est la valeur initiale du signal à l'instant t_0
et $\mu = \lambda . b/k$

La figure ci-contre donne l'allure du signal transmis suite à deux créneaux de vitesse de rotation. On constate que le signal suit sensiblement les variations rapides de **Ω**, mais qu'une fois **Ω** constant, le signal s'amortit, si bien que l'arrêt de la rotation se traduit par un signal correspondant à une rotation inversée suivi d'un retour lent au zéro. C'est le phénomène bien connu du valseur qui une fois à l'arrêt, voit la salle tourner à l'envers.

FIN